# CHAPTER *2*

# COMMUNICATIONS ADMINISTRATION

## LEARNING OBJECTIVES

*Upon completing this chapter, you should be able to do the following:*

- *Identify the background and mission of the departments within the National Communications System.*

- *Identify the mission and policy of naval communications.*

- *Identify the functions of the Naval Telecommunications System and the roles of communications management personnel.*

- *Identify the elements and responsibilities related to standard message processing.*

- *Identify the procedures for minimize consideration and processing of messages.*

- *Identify the procedures used for general administration and handling of communication files.*

- *Identify the procedures used in communications planning.*

- *Identify the procedures for conducting watch-to-watch inventories and updating the NWPs.*

- *Identify the role of the naval warfare publications library (NWPL) including NWPL administration and maintenance.*

---

"Naval communications" is the term assigned to the entire communications effort of the Department of the Navy, both afloat and ashore. The naval communications complex is the total of all Navy-operated communications installations and services. The communications complex provides, operates, and maintains tactical communications, including fleet broadcast, ship to shore, and air to ground. The operating forces and all commands and activities ashore depend on this complex for reliable transmission and receipt of information.

In this chapter, we will give you a broad overview of how naval communications is organized at shore commands and aboard ship. We will also discuss the various publications used in naval communications. These publications provide standard guidance for all phases of naval communications, such as basic communications doctrines, message preparation, and proper circuit discipline.

## NATIONAL COMMUNICATIONS SYSTEM

The National Communications System (NCS) was established to achieve a cohesive effort in the event of war. The NCS provides a unified governmental system that links together the communications facilities and

components of the various Federal agencies. Essentially, all branches of the Federal Government, both civilian and military, are part of the NCS. Each department and branch, however, has its individual organization, methods, and procedures.

## DEFENSE COMMUNICATIONS SYSTEM

The Defense Communications System (DCS) exists to support the three military departments (Navy, Army, Air Force) and other Department of Defense activities. The circuits that make up the DCS are government-owned or leased and are point-to-point circuits that are long-haul and worldwide. The DCS combines many of the communication elements of the three military forces into a single communications system.

Although the Naval Telecommunications System (NTS) and the DCS are two different communications systems (fleet and ashore, respectively), they are constantly intermixed. For example, as often happens, a naval message originated aboard ship and destined for a shore activity leaves the ship over the NTS, but final routing is accomplished over the DCS circuits. The interface between the NTS and DCS is always provided by the shore communications facility.

## DEFENSE INFORMATION SYSTEMS AGENCY

The Defense Information Systems Agency (DISA) gives operational direction to the DCS. With reference to the DCS, the DISA must ensure that the system is operated and improved so as to meet the continual long-haul, point-to-point requirements that arise.

The DISA functions under the management of a director who is appointed by the Secretary of Defense. The director is a flag-rank officer and is responsible for coordinating the combined communications elements of the three military departments.

## MISSION OF NAVAL COMMUNICATIONS

The mission of naval communications is to provide and maintain reliable, secure, and rapid communications, based on war requirements, to meet the needs of naval operating forces. Naval communications must also satisfy the requirements of the Defense Communications System (DCS) and the National Communications System (NCS).

Naval communications must always be ready to shift to the requirements of wartime. Our peacetime organization and training must be capable of making this shift rapidly and with a minimum of changes. Without this capability, our forces would be severely handicapped, and vital defense information would never reach its destination. For this reason, we have a well-defined communications structure, with responsibilities assigned to each element, from the Chief of Naval Operations (CNO) down to individual fleet units.

## POLICY OF NAVAL COMMUNICATIONS

The policy of naval communications is to:

- Establish and maintain effective communications within the Department of the Navy;

- Encourage at all levels of command an effort to improve techniques, procedures, and efficiency;

- Cooperate with the military services, Defense Information Systems Agency (DISA), and other departments and agencies of the U.S. Government and allied nations;

- Encourage development of the amateur and commercial communications activities of the United States to enhance their military value and to safeguard the interests of the nation; and

- Promote the safety of life at sea and in the air by maintaining communications facilities with the U.S. Merchant Marine, aircraft over sea, and appropriate U.S. and foreign communication stations.

## NAVAL TELECOMMUNICATIONS SYSTEM

The word "telecommunications" includes all types of information systems in which electric or electromagnetic signals are used to transmit information between or among points. The Naval Telecommunications System (NTS) is comprised of all the end terminal processing equipment, transmission, switching, cryptographic, and control devices used to transmit operational information in the Navy.

The NTS provides electrical and optical communications from the commander in chief and naval commanders down to all naval forces under its command. You should remember that the NTS is used primarily to exercise command and control over the naval operating forces; not the shore establishment. Most shore establishments are served through the Defense Communications System (DCS). Naturally, there are overlapping portions of each system where necessary.

Operational direction and management control of the assigned elements of the NTS are the responsibility of the Commander, Naval Computer and Telecommunications Command (COMNAVCOM-TELCOM).

In naval communications, COMNAVCOM-TELCOM determines the responsibilities of each of the various commanders, whether a fleet commander or the commanding officer of a ship. For example, direction and control of all naval fleet broadcasts, ship shore, air-ground, and other direct fleet-support telecommunications are assigned to the fleet commanders in chief. That is to say, all Pacific Fleet naval broadcasts are under the operational direction and control of the Commander in Chief, Pacific Fleet (CINCPACFLT). The same applies to Atlantic Fleet navak broadcasts. These broadcasts are under the operational direction and control of the Commander in Chief, Atlantic Fleet (CINCLANTFLT).

Fleet commanders in chief are responsible for the adequacy of communications to satisfy the needs of their respective fleets. They, in turn, assign broad communications responsibilities in the form of fleet operation orders (OPORDs). OPORDs are to be complied with at every level down through individual commanding officers of operating ships.

The commanding officers use only those portions of the fleet commander's communications OPORD that affect them. In this simple, yet direct, manner, the NTS is administered at every operational level in the fleet, according to that ship's mission and communication needs. We will talk more about OPORDs later in this chapter.

The Naval Telecommunications Command is composed of the following elements:

- Commander, Naval Computer and Telecommunications Command (COMNAVCOMTEL-COM);

- Naval Computer and Telecommunications Area Master Stations (NCTAMSs);

- Naval Computer and Telecommunications Stations (NAVCOMTELSTAs, sometimes referred to as NCTSs);

- Naval Communications Detachments (NAVCOMTEL DETs, also abbreviated NCTDs);

- Naval Data Automation Commands (NAV-DACs);

- Naval Security Group Departments (NAV-SECGRUDEPTs) of NAVCOMTELSTAs; and

- Navy-Marine Corps Military Affiliate Radio System (MARS).

## COMMANDER, NAVAL COMPUTER AND TELECOMMUNICATIONS COMMAND

With the merging of Automated Information Systems (AIS) and telecommunications, the mission and responsibilities of COMNAVCONTELCOM have greatly increased. You will see COMNAVCOM-TELCOM continue to change and grow as telecommunications technology advances into the 21st century.

There have already been changes in the makeup of the COMNAVCOMTELCOM claimancy as communications stations have merged with Naval Regional Data Automated Centers (NARDACs). Those communications stations that do not merge with an AIS activity will become Naval Computer and Telecommunications Stations (NCTSs) or Naval Computer and Telecommunications Detachments (NCTDs).

Although not all-inclusive, COMNAVCOMTEL-COM's responsibilities include the following:

- Integrates and consolidates Navy common-user ashore communications and information resources (IR) (including personnel) into the NAVCOMTELCOM claimancy, and implements Navy IR management policy within the claimancy;

- Advises the Director, Naval Space and Warfare Command, of validated communications requirements that may demand development or modification of satellite communications systems;

- Formulates policy on, and exercises authoritative control over, the Navy Communications Security Material System (CMS), and reviews or initiates action in cases of loss or compromise of CMS material;

- Serves as Department of the Navy (DON) manager of leased portions of Navy dedicated and common-user information transmission systems;

- Manages the Navy and Marine Corps Military Affiliate Radio System (MARS) and coordinates Navy participation in amateur radio matters;

- Establishes, implements, and maintains the Fleet Operational Telecommunications Program;

- Manages International Maritime Satellite (INMARSAT) communications ground interfaces to naval communications for the DON and handles any other commercial telecommunications authorized by law or treaty;

- Operates and maintains the NCTSs, NARDACs, and assigned elements of the Defense Communications System (DCS);

- Serves as technical advisor to CNO for communications/enlisted ratings (RM, ET, and assists in career development and training for these ratings; and

- Serves as central design agency for communications in the DON, performs life-cycle management on Navy Standard Communications Software components.

## NAVAL COMPUTER AND TELECOMMUNICATIONS AREA MASTER STATIONS (NCTAMSs)

As we mentioned earlier, there have been changes in the claimancy of NAVCOMTELCOM. As a result, each of the former NAVCAMS has been redesignated as a NCTAMS, and has merged with a NARDAC. The four NCTAMSs are NCTAMS EASTPAC, Honolulu, Hawaii; NCTAMS LANT, Norfolk, Virginia; NCTAMS WESTPAC, Guam; and NCTAMS MED, Naples, Italy.

The world is divided into four Naval Communications Areas (NAVCOMMAREAs): Western Pacific (WESTPAC), Eastern Pacific (EASTPAC), Atlantic (LANT), and Mediterranean (MED) (figure 2-l). All communications activities within any of these geographical areas are organized to operate under the operational control of a NCTAMS. These master stations are the major sites in a COMMAREA and are the primary keying stations for that area. They are the entry points for Navy Tactical Satellite Systems and also operate and maintain one or more Defense Satellite Communications System (DSCS) terminals.

The NCTAMSs have, as part of their organization, a fleet telecommunications operations center (FTOC). This is the focal Point for fleet communications support.

To support the operating forces of each fleet commander in chief (FLTCINC), the authority to exercise operational direction over all NAVTELCOMs is delegated on an area basis to the commanding offiers of the master stations. Operational direction is decentralized down to the commanding officers of the NCTAMSs. These commanding officers report to and are immediately responsible to the FLTCINC. COMNAVCOMTELCOM, however, exercises overall operational direction to assure integration of the worldwide system, taking into consideration the requirements and priorities of other FLTCINCs and/or higher authority. You should refer to the appropriate Fleet Operational Telecommunications Program (FOTP) manual for futher information.

Within the various NAVCOMMAREAs are alternate NCTAMSs. They coordinate control of communications under the direction of the primary NCTAMSs.

## NAVAL COMPUTER AND TELECOMMUNICATIONS STATION

A Naval Computer and telecommunications Station (NAVCOMTELSTA) is a communications station with the primary responsibility for communications in a large specific area. This responsibility includes all communications facilities and equipment required to provide essential fleet support and fixed communications services. For example, NAVCOMTELSTA, Diego Garcia, serves a large geographical area of the Pacific and Indian oceans. It also includes facilities and equipments necessary to interface with all other NAVCOMTELSTAs or
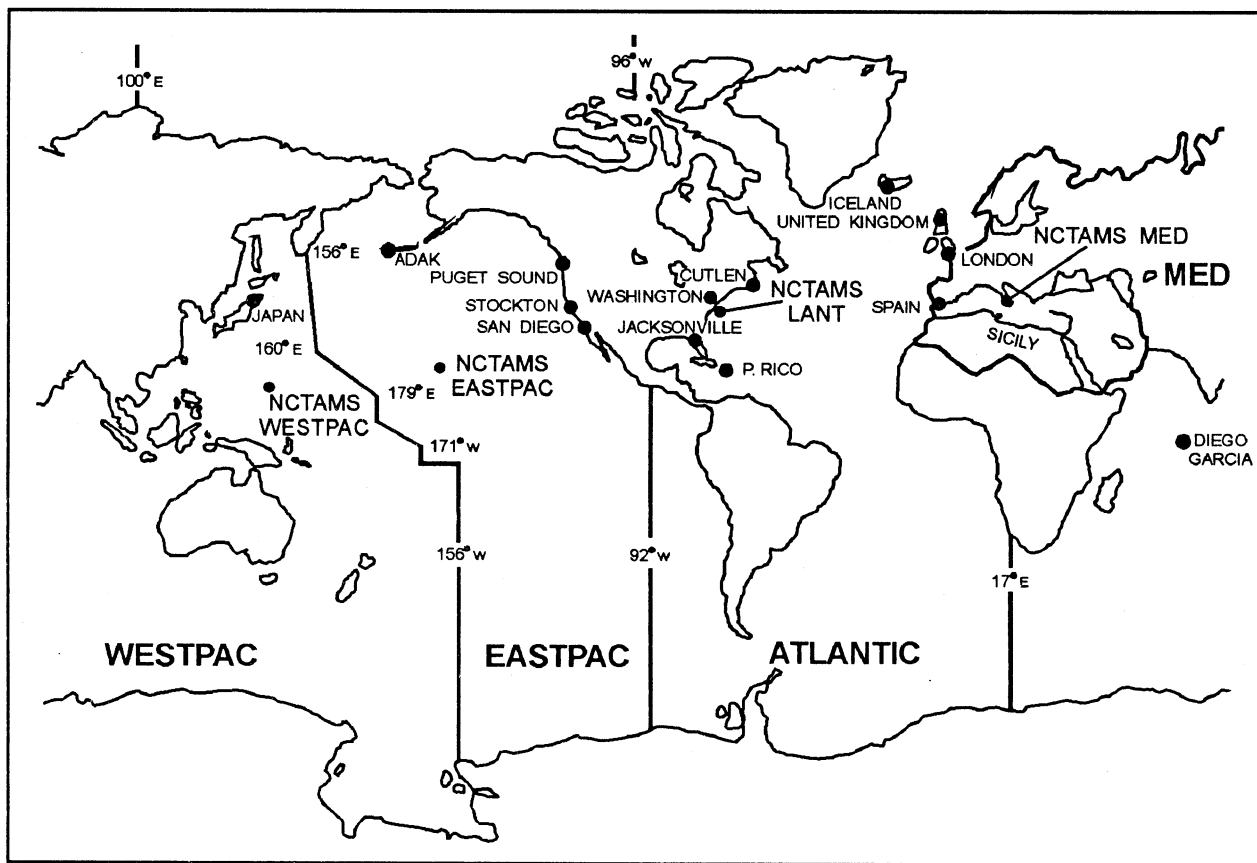
Figure 2-1.—Naval communications areas.

communications detachments on all naval communications matters. It also provides Naval Industrial Fund (NIF) AIS services to Navy customers.

## NAVAL COMPUTER AND TELECOMMUNICATIONS DETACHMENT

A Naval Computer and Telecommunications Detachment (NAVCOMTELDET) is a small telecommunications facility that is assigned a limited, or specialized, mission and has a limited number of personnel and facilities.

## NAVAL DATA AUTOMATION FACILITY

A Naval Data Automation Facility (NAVDAF) comes under the control of an NCTS or a NARDAC. NAVDAFs provide AIS services in areas where no NARDACs are located. The workload of a NAVDAF is normally less than that of a NARDAC.

## NAVAL SECURITY GROUP DEPARTMENTS

The Naval Security Group Departments (NAVSECGRUDEPTs) come under the authority of Commander, Naval Security Group Command (COMNAVSECGRU), and are responsible for the cryptologic and related functions of the Navy. NAVSECGRUDEPTs maybe part of a NCTAMS or a NAVCOMTELSTA. As such, COMNAVSECGRU exercises technical control over the cryptologic operations, whereas COMNAVCOMTELCOM has overall responsibility for the management and operating efficiency of the NAVSECGRUDEPTS.

## MILITARY AFFILIATE RADIO SYSTEM (MARS)

A function of the Military Affiliate Radio System (MARS) is to provide auxiliary communications to military, civil, and/or disaster officials during periods of emergency. The Navy encourages amateur radio operators to affiliate with MARS. Many of the

operators have earned their amateur radio licenses from the Federal Communications Commission.

The amateur radio operators, using their amateur stations on Navy radio frequencies, receive training in naval communications procedures and practices. Besides assisting in emergency situations, MARS operators also create interest and furnish a means of training members in naval communications. You can find detailed information about the MARS program in *U.S. Navy-Marine Corps Military Affiliate Radio System (MARS) Communications Instructions,* NTP 8.

## NAVAL COMMUNICATIONS MANAGEMENT

As radiomen advance, they can expect to assume additional authority and responsibility. A first class or chief will most likely be placed in charge as a watch supervisor, leading petty officer or chief, or even as a division officer. These are only a few of the many leadership positions to which they might be assigned. In summary, eventually, a career Radioman is going to be a manager.

The Navy has conducted extensive studies to pinpoint problems in the area of communications organization and management. These were done to allow communications personnel to take corrective action on the problem areas. Use of sound managerial principles helps us accomplish our mission.

All levels of management require an evaluation standard. Managers are then able to properly evaluate specific communication systems or components. Such an evaluation provides a basis for comparison of equipment, personnel, and even complete facilities. This evaluation forms the basis for establishing additional standards and guidelines. A continuing evaluation requires data collection via a system of feedback reports from all managerial levels.

### EVALUATING PERFORMANCE

Effectiveness of naval communications is the first consideration in the management of any communications facility. The overall capability must be viewed in relation to each functional unit. Standards of performance can be established and control elements determined. An evaluation of the entire system must be completed by the highest level of command. Each operational unit must be scrutinized by the chief or first class in charge.

### Establishing Standards

Standards of performance must be established to determine the effectiveness of operations and service provided against customer requirements and system capability. Standards must be established for internal functions as well as for overall system performance. After performance standards are established, the control elements and manner of control can be determined.

It is most important that performance standards be established in the general areas of reliability, speed, security and economy. These areas can be broken down into standards for internal operation, equipment, personnel, maintenance, supply, and so forth.

Realistic standards of performance must be established. This allows maximum use of resources without overcommitment. The standards must be compatible with command requirements and within resource capability. The standards must also be flexible enough to allow for changing operating conditions. Skill levels and manning levels change constantly. Equipment status and configurations are never stable. Operating conditions and commitments change from day to day. Therefore, each communications facility manager must establish flexible standards to accommodate changing requirements and situations.

### Management Responsibilities

Mid-management radiomen must realize the need for progressively improving standards. The following points may assist mid-management radiomen in improving standards within their division:

- **Overcoming Resistance—** The practice of relying on past performance as a basis for establishing standards is often sound. With an organized effort, however, conditions can be changed to improve performance. If the personnel responsible for better performances participate in the organized effort, the problem of resistance to higher standards is often eliminated.

- **Improving Conditions—** Owing to the rapid growth and change in the character of communications systems, considerable managerial effort must be devoted to improving the effectiveness of operations and service. The essential approach to this type of problem can be summarized in a sequence of three stages:

  — Discovery of the problems; that is, what part of an existing condition needs improving;

— Diagnosis to determine what changes are needed to bring about the needed improvement; and

— Remedial action; that is, implementing the necessary changes.

- **Responsibility**— Responsibilities must be established in accordance with the organizational structure and be clearly defined.

- **Organizational Considerations**— Leading radiomen must realize that the existing organizational structure may be a contributing factor to poor personnel performance. In such instances, recommendations to realign the organizational structure must be seriously considered.

- **Conservation of Personnel Resources**— The communications facilities manager must be constantly aware of the need to conserve personnel resources at all levels. Conservation of personnel resources is accomplished by evaluating personnel requirements properly and by using available personnel effectively through proper training and assignment.

## GENERAL ADMINISTRATION

A communications facility should function effectively and efficiently. This is normally the result of the senior supervisor's ability to set up and manage the organization.

Good supervisors retain open minds. They recognize the need for change and implement those changes as required. They acquire a thorough knowledge of the functions performed by their area of responsibility and understand how it relates to the overall mission. Only then can they plan a rational approach to correct a problem or make positive changes.

Although the current structure and methods may meet the objectives of the division, a periodic review should still be conducted. The goal is to develop more efficient office methods, techniques, and routines. Procurement of state-of-the-art equipment may require a complete evaluation and reorganization of divisional workflow and workspace layout. To plan properly, the supervisor must know the following information:

- **WHAT** work is to be done;

- **WHY** the work is to be performed;

- **WHEN** the work is to be performed;

- **HOW** the work is to be accomplished;

- **WHERE** the work is to be performed; and

- **WHO** is responsible for completing the work.

## PERSONNEL MANAGEMENT

Good managerial traits and supervisory abilities are prerequisites for the first class or chief petty officer who is required to function as a front line supervisor and manager. The RM1 or RMC will normally be the RM supervisor and will have many managerial and supervisory responsibilities added to those present at the junior petty officer level.

Supervision involves working with people, and a major responsibility of a supervisor is production. A good supervisor knows how to get a job done by getting the most out of personnel. However, the desire to attain an acceptable production level must not be at the expense of personnel assets. People have the right to be treated as individuals and respected as such. If treated in any other reamer, no amount of pressure will create a permanent increase in production levels. While you want to achieve a high level of production, you also want your personnel to produce willingly and be interested in their work.

## OFFICE MANAGEMENT

The physical location of a communications office is normally predetermined by higher authority. Furthermore, the space allotted to the various sections is usually determined by competent engineers based on available space. After discussing the matter with the senior petty officers in the division, the division officer or division chief usually determines the physical location of furniture and equipment.

When the office layout is being planned, primary consideration must be given to proper flow of paper and work, the physical location of workspaces, and the internal communications of the division.

Secondary factors to be considered are the number of personnel to be accommodated, safety standards, security of classified material, structural location of electrical outlets, and physical locations of bulkheads and passageways.

### Paper and Work Flow

Good paper flow is the smooth movement of paperwork from one desk or individual to another. As much as possible, the paperwork should flow in one direction through various sections with no reversals or

criss-crossing. Figure 2-2 shows the ideal communications space layout with sequential workflow. Placing related tasks in adjacent spaces reduces distance and increases efficiency of operations. This ultimately increases the work accomplished.

Workflow affects the placement of sections within the division and the location of desks, files, and other equipment. Changes should only be made to improve workflow. Deviations from approved methods can result in loss of time and motion and cause delays in completion of work assignments.

**Physical Factors**

The physical layout of workspaces should be reviewed when:

- There is evidence of improper workflow;

- The number of personnel or office procedures change;
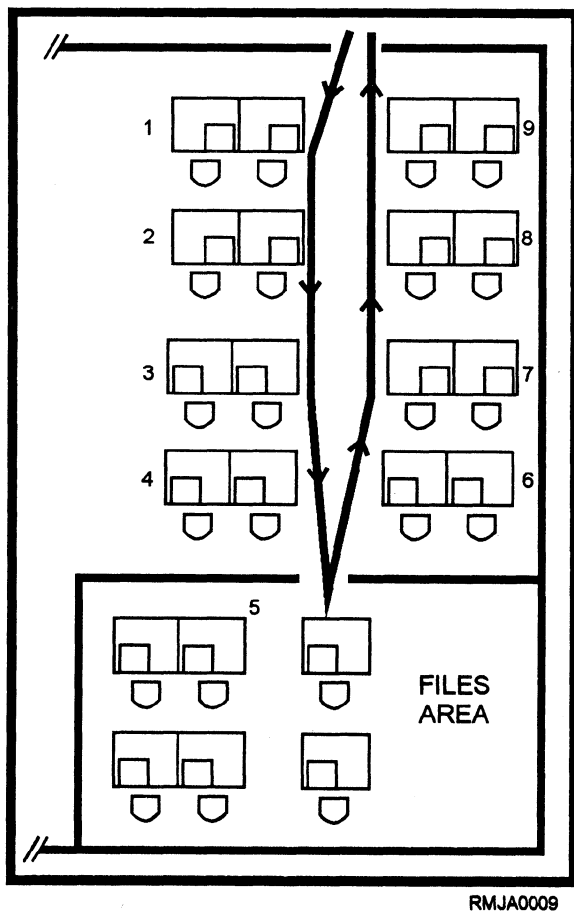
- The volume of work increases or decreases;



Figure 2-2.—Ideal communications space layout.

- New equipment is ordered or is to be installed; or

- There is a change in allotted space.

Before actually moving personnel or equipment, it is a good idea to draw a scale model of the anticipated layout. You can then evaluate the idea and judge its effectiveness.

In evaluating an office layout, you should consider the following factors:

- Office congestion;

- Personnel supervision;

- Use of space;

- Volume of work versus people; and

- Office appearance.

**Internal Communications**

A large portion of communications office work consists of receiving, distributing, and filing communications, reports, instructions, and records. Another major portion of the work is the disposition of correspondence. When handling correspondence, the supervisor must establish standard procedures. Once decided, these procedures should be conveyed both vertically and horizontally. Vertical communications are routed up and down the chain of command. Horizontal communications are routed to other divisions and departments.

Vertical communications can be either formal or informal. Formal information usually consists of office procedures, watches, schedules, job instructions, and written orders. Formal communications are handled to ensure wide dissemination and accuracy of information, to avoid distortions, and to provide a permanent record. Informal information is usually passed orally and provides guidance and instructions on work assignments.

Horizontal communications can be either formal or informal. Personnel holding parallel positions (two watch supervisors for instance) can sometimes resolve problems through informal communications without involving higher authority. On the other hand, formal communications must be used when the subject requires approval through the chain of command. Formal communications may be in the form of station directives, administrative procedures, or station watch bills.

# COMMAND COMMUNICATIONS ORGANIZATION

The structure of the communications organization of a command depends on command size and whether the command is ship- or shore-based. Not all Navy ships have a communications department. *Basic Operational Communications Doctrine (U),* NWP 4 (NWP 6-01), designates the types of ship that should have a communications department. In ships that are not so designated, communications personnel are assigned to the operations department, but the communications functions are the same as those for ships with a communications department. Future organization may structure communication and automated systems into a combined information systems department.

Senior enlisted personnel may be assigned communications duties normally assigned to officers if there are insufficient officers to fill communications billets. Figure 2-3 shows a normal shipboard communications organization. Key billets are further discussed in this chapter.

## Commanding Officer

The commanding officer of a ship or a shore command is responsible for the communications of that command. The only exception to this is when a flag officer is embarked aboard a ship, making that vessel the flagship. In such cases, the embarked commander assumes control of flagship communications. The commanding officer is still responsible for the proper handling of message traffic within the ship.

## Communications Officer

The communications officer (COMM officer) is responsible for the organization, supervision, and coordination of the command's exterior communications. At shore stations, the COMM officer is the department head. Aboard ship, the COMM officer may be assigned as a department head or may be assigned under the operations officer. Aboard ship, the COMM officer is also responsible for the management of related internal communications systems.

## Radio Officer

The radio officer is in charge of the communications center. This officer is responsible for organizing and supervising assigned personnel to ensure accurate, secure, and rapid communications. The radio officer is responsible to the communications officer for:

● Preparing the command's communications plan;
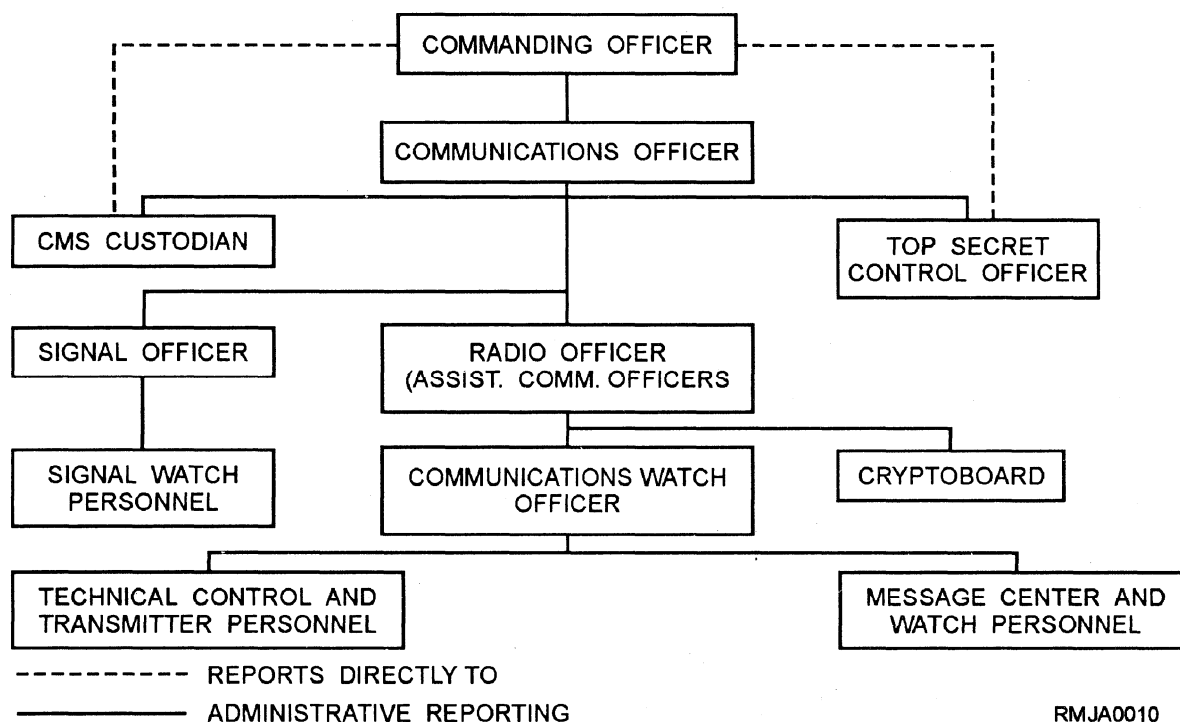


Figure 2-3.—Communications organization.

- Monitoring the proper allocation of equipment for operations;

- Preparing and maintaining the communications watch, quarter, and station bill;

- Conducting the communications training program; and

- Preparing standard operating procedures (SOPs) for the communications center.

On small ships, the communications officer and the radio officer maybe the same person.

## Communications Security Material System (CMS) Custodian

The CMS custodian is responsible to the commanding officer for:

- Managing the CMS account in accordance with the instructions contained in the *Communications Security Material System (CMS) Policy and Procedures Manual,* CMS 1;

- Advising the commanding officer on matters concerning the physical security and handling of CMS publications and materials;

- Stowage of CMS publications and materials, as well as the drawing, correcting, and authorized destruction; and

- Submitting all reports concerning the accountability and issuance of CMS publications and materials.

## Watch Section Personnel

The functions of the operational organization of a communications command consist of:

- Message processing, circuit operation, technical control, data processing, and operation; and

- Control of voice circuits and the operation of satellite circuits, where installed.

The combined efforts of the operational organization are performed in various spaces simultaneously. In the next section, we will discuss the duties and responsibilities of some of the key billets within this organization.

**COMMUNICATIONS WATCH OFFICER (CWO).—** The CWO is responsible to the communications officer for:

- Ensuring that communications capabilities are accomplished in accordance with the command's mission;

- Incoming and outgoing traffic, ensuring that all messages, transmitted or received, are handled rapidly and accurately in accordance with existing regulations; and

- Ensuring compliance with existing communications directives and monitoring the performance of on-watch personnel and spaces.

*Fleet Communications (U),* NTP 4, contains a detailed listing of the duties of the CWO.

**SENIOR WATCH SUPERVISOR (SWS).—** When assigned, the SWS is the senior enlisted person on watch in communications spaces and is responsible to the CWO for:

- The proper handling of all communications;

- Notifying the CWO on all matters of an urgent or unusual nature;

- Examining operational logs and monitoring equipment alignment and operation; and

- Directing action necessary to prevent or overcome message backlogs.

In addition to the duties listed in NTP 4, the SWS is also responsible for any other duties as maybe assigned by the CWO.

**COMMUNICATIONS CENTER SUPERVISOR.—** The communications center supervisor is responsible to the CWO and SWS for:

- Supervising message processing and circuit operations;

- Directly supervising all radiomen on watch in the message processing center; and

- Notifying the CWO and SWS on all matters of an unusual or urgent nature.

**TECHNICAL CONTROL SUPERVISOR.—** The technical control ("tech control") supervisor is responsible to the CWO for:

- Establishing and maintaining required circuits, and initiating action to restore or bypass failed equipment;

- Ensuring that quality monitoring and control procedures are used on all systems;

- Maintaining the status board showing pertinent information on all equipment, nets, and circuits in use; and

- Directly supervising all personnel assigned to technical control and transmitter room spaces.

## Command Ship Communications

The term "flagship" is sometimes used instead of "command ship" but means the same thing. Either term means that a group, squadron, or division commander is embarked on board, thereby making that vessel the flagship, or command ship. We mentioned earlier that, in flagships, the embarked commander assumes responsibility for communications functions. The flag communications officer is responsible for ship and flag communications requirements. However, the internal routing of message traffic remains the responsibility of the commanding officer of the ship in which the flag is embarked.

When a flag officer is embarked, the ship's communications officer, communications watch officers, and enlisted communications personnel may be ordered to additional duty in the flag communications division. These personnel are directly responsible to the flag communications officer for the operation of the flag communications functions. The ship's communications officer reports to the flag communications officer and is the contact officer for matters pertaining to the handling of ship and staff message traffic. Figure 2-4 illustrates a standard watch organization aboard a ship with a flag embarked.

By now, you should have a basic idea of how naval communications is organized at shore commands and aboard ship. Remember that there are variations in all organizations. The command size, scope of operations, and personnel assets are just a few of the factors that affect the structure of the communications organization.

## OPERATION ORDERS

Operation orders (OPORDs) are directives issued by naval commanders to subordinates for the purpose of effecting coordinated execution of an operation.
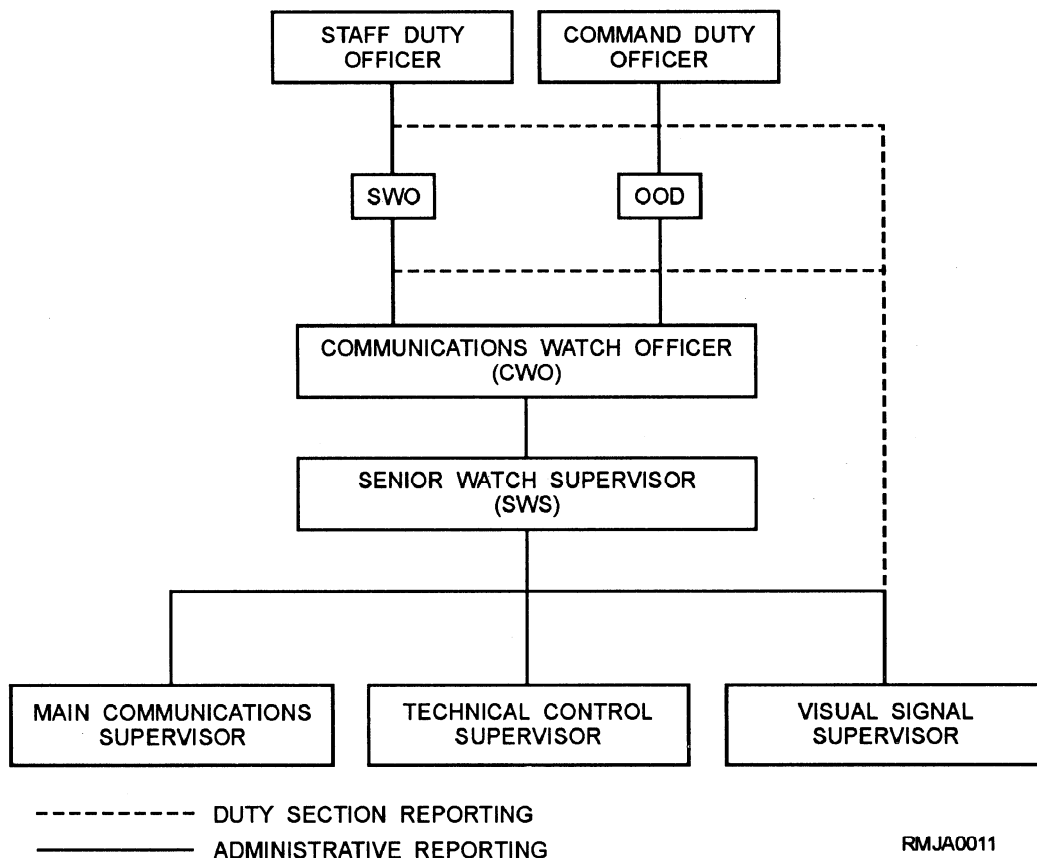


Figure 2-4.—Communications watch organization.

Operation orders are prepared in accordance with a standing format, as set forth in *Naval Operational Planning,* NWP 11 (NWP 5-01).

An OPORD is an operations plan made up of the heading, body, and ending. The basic plan, contained in the body of the OPORD, is concise and contains minimum detail. More detailed information on various ship departments is contained in enclosures (called annexes and appendixes).

The annex of most concern to radiomen is the communications annex. The communications annex, along with its appendixes and tabs, discusses the many details to be considered in planning communications for a particular operation. In this annex, you can find such information as the applicable circuits, equipment, and frequencies that will be used in the upcoming operation.

## STANDARD OPERATING PROCEDURES

In addition to the OPORDs, you should also become familiar with the standard operating procedures (SOPs) used by your division and department. SOPs should be sufficiently complete and detailed to advise personnel of routine practices. The detail depends upon such variables as the state of training, the complexity of the instructions, and the size of the command.

Staff sections, divisions, and departments often find it convenient to establish their own SOPs for operating their respective areas and for guiding their personnel in routine matters. Some examples of communications SOPs are:

- Procedures for persons going aloft;

- Handling of visitors in radio spaces; and

- MINIMIZE procedures.

Communications SOPs are written to meet an objective. SOPs may vary from command to command and may differ according to their objectives. Your job will be to recommend changes or maybe even write the objectives. In any event, a complete set of SOPs will enable you and your shipmates to perform your duties in a responsible, professional, and safe manner.

## MESSAGE LOGS

Accounting for messages addressed to your guard list (list of commands for which you receive message

traffic) is the most important part of processing messages. Accounting for all messages processed in your message center is accomplished with logs. Although ashore and afloat automated systems automatically log, store, and retrieve messages, there still is a need to manually log and file both incoming and outgoing messages.

## CENTRAL MESSAGE LOG

Depending upon the traffic volume processed, a message center may use either a separate outgoing/incoming log or a combined Central Message Log to record processed message traffic. All messages are logged in the Central Message Log after they have been logged in the appropriate circuit log. The normal practice is to use separate logs for outgoing and incoming messages (figure 2-5).

The entries in the Central Message Log are station serial number (SSN), precedence, DTG (original on a readdressal), originator (original on a readdressal), subject, classification, time of receipt (TOR) for incoming messages or time of delivery (TOD) for outgoing messages for each message. It is also useful to indicate on the log over which circuit the message was relayed. This is helpful during tracer situations. The Central Message Log is filed in the communications center master file on top of the messages processed for that radio day (raday).

## TOP SECRET CONTROL LOG

Upon receipt of a Top Secret message, including SPECAT SIOP-ESI, addressed to the parent command or subscriber of the message center, the center assigns a sequential number and enters the originator, DTG, and copy count of the message into the Top Secret Control Log. A separate entry is made for each addressee. The messages must be annotated as "Copy ___ of ___" and "Page ___ of ___." The message must also be assigned a Top Secret control sequential number.

## CIRCUIT LOGS

Records of messages sent via ship-shore circuits, whether primary shipshore, full-period termination, and soon, must be maintained. This ensures continuity of traffic, accurate times of delivery/receipt, and precise files for possible tracer action. These actions should be recorded on the Received Message Record, OPNAV

DATE _____

# CENTRAL MESSAGE LOG

## OUTGOING / INCOMING

| SSN | PREC | DTC | ORIG | SUBJ | CLASS | TOR | TOD | CKT |
|-----|------|-----|------|------|-------|-----|-----|-----|
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |
|     |      |     |      |      |       |     |     |     |

RMJA0012

Figure 2-5.—Central Message Log for outgoing and incoming messages.

**RECEIVED MESSAGE RECORD**
OPNAV FORM 2110-15 (Rev. 11-58)

(Reorder from FPSO
Cog. "I" Stock)

| CIRCUIT | DATE | CARD NO. |
|---|---|---|

S-T

| 51 | | 76 | |
|---|---|---|---|
| 52 | | 77 | |
| 53 | | 78 | |
| 54 | | | |
| 55 | | | |
| 56 | | | |
| 57 | | | |
| 58 | | | |
| 59 | | | |
| 60 | | | |
| 61 | | | |
| 62 | | | |
| 63 | | | |
| 64 | | | |
| 65 | | | |
| 66 | | | |
| 67 | | | |
| 68 | | | |
| 69 | | | |
| 70 | | | |
| 71 | | | |
| 72 | | | |
| 73 | | | |
| 74 | | | |
| 75 | | | |

BACK

**RECEIVED MESSAGE RECORD**
OPNAV FORM 2110-15 (Rev. 11-58)

(Reorder from FPSO
Cog. "I" Stock)

| CIRCUIT | DATE | CARD NO. |
|---|---|---|

S-T

| 1 | | 26 | |
|---|---|---|---|
| 2 | | 27 | |
| 3 | | 28 | |
| 4 | | 29 | |
| 5 | | 30 | |
| 6 | | 31 | |
| 7 | | 32 | |
| 8 | | 33 | |
| 9 | | 34 | |
| 10 | | 35 | |
| 11 | | 36 | |
| 12 | | 37 | |
| 13 | | 38 | |
| 14 | | 39 | |
| 15 | | 40 | |
| 16 | | 41 | |
| 17 | | 42 | |
| 18 | | 43 | |
| 19 | | 44 | |
| 20 | | 45 | |
| 21 | | 46 | |
| 22 | | 47 | |
| 23 | | 48 | |
| 24 | | 49 | |
| 25 | | 50 | |

FRONT

RMJA0013

Figure 2-6.—Received Message Record, OPNAV Form 2110-15.

Form 2110-15 (figure 2-6). Although this form is primarily designed as a record of received messages, only a pen-and-ink change is necessary for its use as a send log.

## JOURNAL LOGS

In most automated systems, all significant system events are entered in a journal log. This log is a chronological record of data processing operations, which may be used to reconstruct a previous or updated version of a file.

All system-level commands entered by an operator are logged. Log entries are usually queued for delivery to a printer as they are generated, but this is optional. However, they are always journaled to a file from which they can be recalled and printed at a later time, as desired. This log gives a system operator or supervisor the ability to review current and previous system events.

In addition, the journal log supports message accountability. The system records the receipt of every formal message and the termination of every formal message delivery that it schedules.
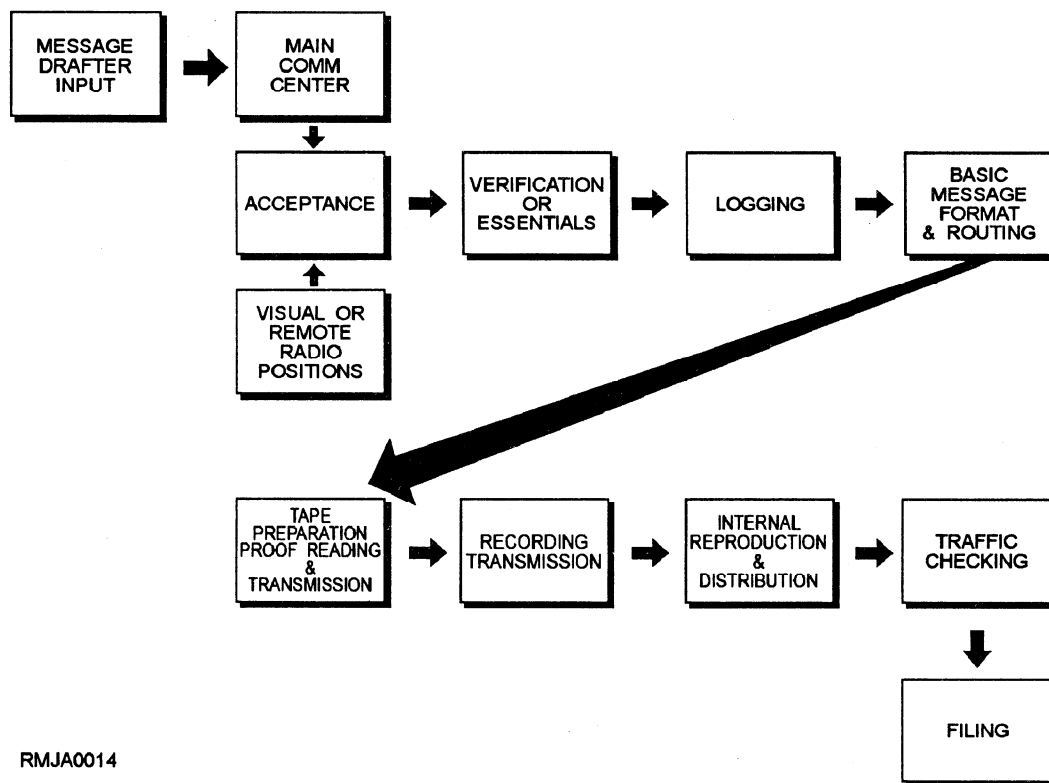
## PROCESSING OUTGOING MESSAGES

Outgoing messages are those messages originated by:

- The command;

- Commands served by the communications center;

- An afloat command if a flag officer is embarked;

- An addressable unit onboard the ship as well as all messages accepted for relay.

The flow chart in figure 2-7 shows the actions required to process outgoing messages.

## HANDLING AUTOMATICALLY PROCESSED OUTGOING MESSAGES

Those messages introduced into the LDMX/NAVCOMPARS from a PCMT, VDT, paper tape reader, data speed reader (DSR), card reader, or magnetic tape are considered "outgoing." They are prepared in JANAP 128, modified ACP 126, or other acceptable formats. Most outgoing messages are destined to be delivered to distant communications centers and commands. Others also have delivery requirements for in-house distribution to commands



RMJA0014

Figure 2-7.—Steps for processing outgoing messages.

2-15

serviced by the communications center. The basic steps for processing outgoing messages are shown in figure 2-8.

The system recognizes whichever format is used upon entry and then validates the start-of-message and end-of-message. After validation, the system outputs either an accept or a reject notice to the operator via the outgoing log. Together with the action notice, the system then outputs a unique header line to identify the message. Accepted messages are assigned a Process Sequence Number (PSN), which is included in the accept notice. They are then stored on diskette for recovery purposes and queued for processing on a first-in, first-out basis by precedence order.

Emergency command or FLASH precedence messages cause any lower precedence messages to be interrupted and a cancel transmission (bust) sequence to be transmitted. The emergency command or FLASH message is transmitted, and normal message processing by precedence is resumed.

Messages are selected for processing based on their precedence and on the order they arrived into the system; first ones in are the first ones processed out. The LDMX/NAVCOMPARS validates the message header and assigns routing indicators (RIs) for delivery as required.

If the system cannot assign an RI automatically, it will display the addressee line to the router VDT. The router may assign the correct RI, place the message on a queue, reject the message from further processing, or correct the short title of the addressee if in error.

A system status containing accounting information pertinent to all the messages on a hold queue will be displayed to the router via the VDT, when the router queue is empty or upon demand by the operator. The router can then retrieve any message on the hold queue by its PSN. If the router rejects the message, the system will record it and print a reject notice on the service log.

Any message determined by the LDMX/NAVCOMPARS system to be duplicated will be rejected to the service printer with the proper annotation.

After all routing is appended to the message, the system assigns the language and media format (LMF)
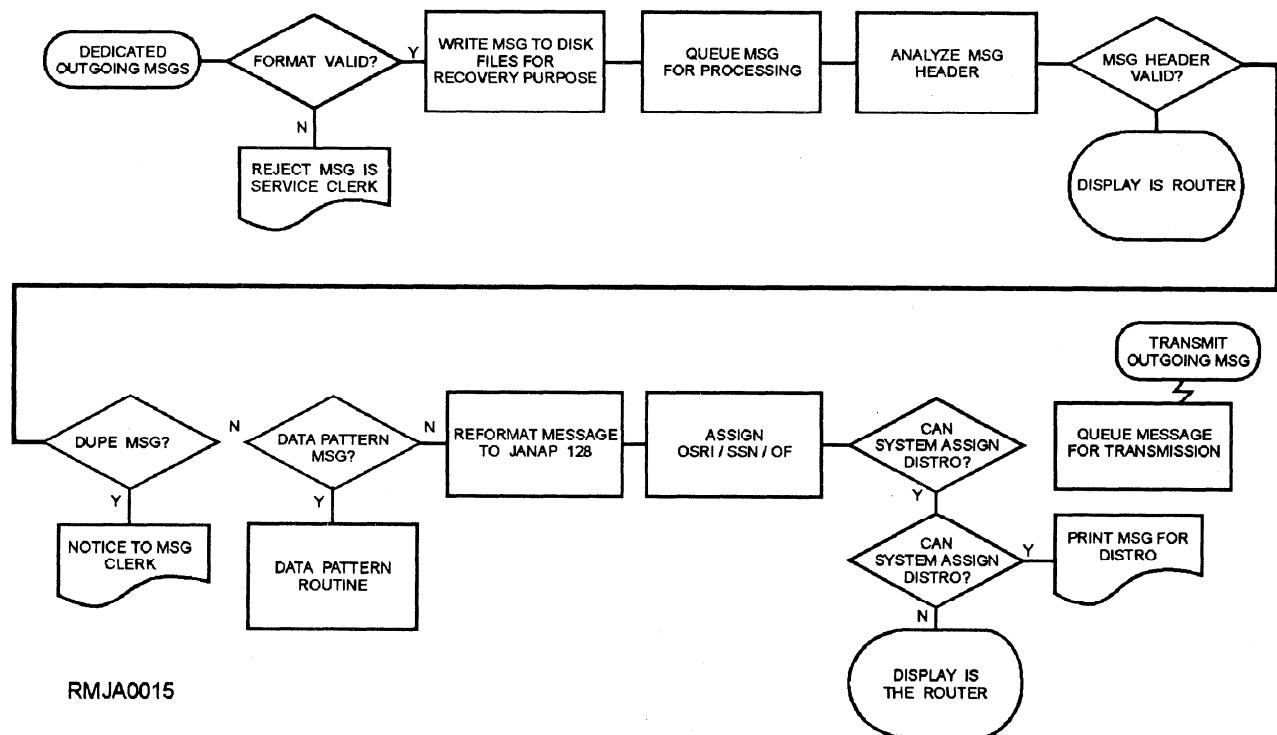


Figure 2-8.—Steps for processing automatic outgoing messages.

(JANAP 128), content indicator code (CIC) (JANAP 128), originating station routing indicator (OSRI), station serial number (SSN), and time of file (TOF) to the message. The message is then paged and sectioned according to JANAP 128, and queued for transmission.

Data-pattern messages may be introduced into the system via card or magnetic tape. The format will be in accordance with JANAP 128 procedures for data messages. During the message preparation, processing, transmission, and filing, the same controls and restraints used for narrative message processing will also apply to data-pattern messages.

The message may also have delivery requirements for distribution to commands serviced by the communications center. The system will automatically assign internal message distribution for all guard commands. If the system cannot provide internal distribution, the message will be displayed to the inrouter for assistance.

## MESSAGE AND ROUTING ADDRESSEES

Most messages have at least one addressee responsible for taking action on the contents and for originating any necessary reply. Addressees who have an official concern in the subject of the message, but who do not have primary responsibility for acting on it, receive the message for information. Although information addressees are usually concerned only indirectly with a message, they occasionally must take action of some kind within their own commands. Some messages contain only information addressees.

Messages may be divided into types, according to the way they are addressed, as follows:

**Single-Address—** A message that has only one addressee, which may be either for action or information.

**Multiple-Address—** A message that has two or more addressees, which may be either action or information and where each addressee is informed of all other recipients.

**Book—** A message destined for two or more addressees but where the drafter considers it unnecessary that each addressee be informed of other addressee(s). Book messages are routed according to each addressee's relay station. All unnessary addressees are deleted from the face of the message before being sent to the addressee(s) served by that particular relay station.

**General Message—** A message that has a wide, predetermined, standard distribution. General messages are normally titled with a sequential number for the current year; for example, ALCOM 28/96, NAVOP 30/96. The title indicates distribution and serves as the address designator.

## ADDRESS GROUPS

Address groups are four-letter groups assigned to represent a command, activity, or unit. In military communications, address groups can be used in the same manner as call signs to establish and maintain communications. Generally speaking, the Navy uses address groups the same way as call signs. Address groups never start with the letter N; hence, they are easily distinguishable from naval radio call signs. Address groups, however, follow no distinctive pattern, and the arrangement of the four letters that constitute them conveys no significance whatsoever.

Afloat commands (except individual ships) and shore-based commands or activities not served by their own communications facilities are assigned address groups. For example:

- Senior commands and commanders ashore, such as the Secretary of Defense and the Secretary of the Navy;

- Navy bureaus, systems commands, and district commandants; and

- Elements of the shore establishment having a need for direct addressing and receipt of message traffic (such as weather centrals).

Among other uses, address groups facilitate delivery of message traffic when a communications center serves so many activities that its own call sign is insufficient to identify the addressee. Address groups are contained in *Allied Call Sign and Address Group System—Instructions and Assignments,* ACP 100, and in *U.S. Call Sign &Address Group System Instructions & Assignments (U.S. Supplement No. 1),* ACP 100 U.S. SUPP-1. Like call signs, address groups are divided into the following types:

- Individual activity;

- Collective;

- Conjunctive;

- Geographic;

- Address indicating; and

● Special operating.

## Individual Activity Address Groups

Individual activity address groups are representative of a single command or unit, either afloat or ashore. For example:

DTCI—COMNAVSURFLANT; and
SSMA—CHIEF OF NAVAL OPERATIONS (CNO).

## Collective Address Groups

Collective address groups represent two or more commands or activities. Included in this group are commanders and their subordinate commanders. For example:

JTBC—DESRON 6; and
YQHV—SUBRON 16.

## Conjunctive and Geographic Address Groups

Conjunctive and geographic address groups are discussed together because they are interrelated in their usage.

Conjunctive address groups have incomplete meanings and must have geographic address groups added to them to denote a specific command or location. For this reason, conjunctive address groups are used only with one or more geographic address groups. For example, the conjunctive address group XZKW means "All ships present at ___ ." To complete the meaning, it must be followed by a geographic address group.

Geographic address groups are the equivalent of geographical locations or areas. They are always preceded by conjunctive address groups. For example, the address group DEXL could represent Newport, R.I. Therefore, all ships present at Newport would be addressed XZKW DEXL.

## Address Indicating Groups

Address indicating groups (AIGs) represent 16 or more specific and frequently recurring combinations of action and/or information addressees. The purpose of AIGs is to increase the speed-of-traffic handling. They shorten the message address by providing a single address group to represent a large number of addressees. This eliminates individual designators for each address used in the heading.

Messages that are repetitively addressed to a constant group of 16 or more addressees can effectively be processed by an AIG address designator. For example, let's assume that a hypothetical AIG (AIG 31) is used to address SUBMISS/SUBSUNK message traffic by COMSUBLANT to 30 action addressees and 35 information addressees. Since a single AIG (AIG 31) is used, 65 call signs and address groups are eliminated from the heading of the message.

AIGs are normally created when particular types of message traffic become repetitive enough (at least 12 times a year) and are addressed to enough of the same addressees to warrant it. Among such message traffic are:

● Alerts, air defense warnings, operational or emergency actions, and so forth;

● Destructive weather warnings, such as hurricanes and typhoons;

● Logistical transactions and reports;

● Intelligence summaries;

● Movement reports, such as aircraft, ships, and personnel; and

● Notices to airmen (NOTAMs).

A point for you to remember is that an AIG will not be established for groups of addressees numbering fewer than 16. A complete listing of AIGs by number, cognizant authority, and purpose is contained in *U.S. Navy Address Indicating Group (AIG) and Collective Address Designator (CAD) Handbook,* NTP *3* SUPP-1. A partial listing of AIGs, along with specific action and information addressees, can be found in ACP 100 U.S. SUPP 1.

## Special Operating Groups

Special operating groups (SOGs) are four-letter groups that are identical in appearance to address groups. SOGs are provided for use in the headings of messages to give special instructions. However, SOGs are not used unless specifically authorized by CNO. They must always be encrypted. SOGs may be used singly or with encrypted or unencrypted call signs or address groups.

## DISTRIBUTION CLERK

The distribution clerk reproduces copies of the messages according to the routing instruction of the inrouter and outrouter. The distribution clerk is responsible for making the required number of copies

each subscriber requires and slotting the messages into the appropriate subscriber box.

It is important that the clerk remain alert to prevent slotting messages into the wrong box. This could cause an undelivery situation. The distribution clerk, who handles a great number of messages throughout the watch, must be aware of high-precedence messages and ensure that they are reproduced and distributed in a timely manner for immediate pickup by the subscriber. The clerk must also be "up" on the message center's current SOP for handling special and classified messages.

To prevent viewing by unauthorized personnel, certain messages, such as PERSONAL FOR, AMCROSS, and classified messages, must be placed in envelopes for pickup by subscribers.

Classified messages are placed in two envelopes; the inner envelope is stamped with the classification and any special-handling markings, and then sealed in accordance with local instructions. The outer envelope is marked with the addressee, originator, and DTG of the message, and then sealed.

After reproducing and distributing a message, the distribution clerk places the original copy into a box for filing by the file clerk. When a message is reproduced from the sole copy of a broadcast message, the original copy or a filler must be returned to the broadcast file. If two-ply paper is used on the circuit, the top copy may be used as the master file copy and the bottom copy retained as the circuit monitor copy.

### COMMON MESSAGE ELEMENTS

Before covering the basic format of military messages, we will first discuss the time system and precedence categories used in naval communications.

### TIME

Time is one of the most important elements in communications. Messages are normally identified and filed by either date-time group or Julian date, depending on the method of transmission.

### Date-Time Group

The date-time group (DTG) is assigned for identification and file purposes only. The DTG consists of six digits. The first two digits represent the date, the second two digits represent the hour, and the third two digits represent the minutes. For example, 221327Z

AUG 96 means the 22nd day of August plus the time in Greenwich mean time (GMT). The dates from the first to the ninth of the month are preceded by a zero. We will talk more about the GMT system shortly.

The DTG designation is followed by a zone suffix and the month and year. The month is expressed by its first three letters and the year, by the last two digits of year of origin; for example, 081050Z AUG 96. The zone suffix ZULU (Z), for Greenwich mean time, is used as the universal time for all messages. The exception is where theater or area commanders prescribe the use of local time for local tactical situations. Radiomen never use 2400Z and 0000Z as the DTG of a message. The correct time would be either 2359Z or 0001Z, as appropriate.

**GREENWICH MEAN TIME.—** In naval communications, the date-time group is computed from a common worldwide standard. To meet the need for worldwide time standardization, the international Greenwich mean time (GMT) system was developed. The GMT system uses a 24-hour clock instead of the two 12-hour cycles used in the normal civilian world.

In the GMT system, the Earth is divided into 24 zones. Zone zero lies between 7 1/2° east and 7 1/2° west of the 0° meridian. The 0° meridian passes through Greenwich, England. The time in this zone (zone zero) is called Greenwich mean time (GMT). The military more commonly refers to this as **ZULU** time. Both names refer to the same standard.

Each time zone extends through 15° of longitude. Zones located east of zone zero are numbered 1 through 12 and are designated minus. To obtain Greenwich mean time, you must **subtract** the zone number in which you are located from local time.

Zones located west of zone zero are also numbered 1 through 12 but are designated plus. These zones must be **added** to the local zone time to obtain GMT. As we will discuss shortly, the 12th zone is divided by the 180th meridian, which is the international date line.

Each zone is further designated by a letter. Letters A through M (J is omitted) designate the eastern, or minus, zones. Letters N through Y designate the western, or plus, zones. The designating letter for GMT is Z (ZULU). The zone number, prefixed by a plus or minus sign, constitutes the zone description. Zones crossing land areas often follow boundaries, natural features, or regional demarcations to keep similar or closely related areas within the same zone.

## CONVERTING GMT AND LOCAL TIMES.—

Most countries have adopted the GMT system. As a Radioman, you will need to be able to convert local time to GMT. To do this, you must understand the GMT system. Figure 2-9 is a chart showing the time zones of the world. Refer to the chart as you study the material in the next paragraphs.

To illustrate converting local time to GMT, assume that we are in zone R and the local time is 1000R (10 a.m.). Referring to the time chart in figure 2-9, you can see that zone R lies west in longitude from zone zero, and is designated plus 5. Therefore, we add 5 hours to the local time, 1000, to find that GMT is 1500Z. To convert GMT to local time, we reverse the process and subtract 5 hours from the GMT (1500Z) to obtain 1000R.

The U.S. military services use the 24-hour system to express time in four-digit groups. The first two digits of a group denote the hour and the second two digits, the minutes. Thus, 6:30 a.m. becomes 0630; noon is 1200; and 6:30 p.m. is 1830. Midnight is expressed as 0000 (never as 2400), and 1 minute past midnight becomes 0001. Remember, to eliminate any possible confusion, never use 0000Z or 2400Z as the date-time group of a message. The correct time would be either 2359Z or 000IZ.

We mentioned earlier that the 12th zone is divided by the 180th meridian. This meridian is the international date line (IDL) (figure 2-9). This is where each worldwide day begins and ends. A westbound ship crossing the line loses a day, whereas an eastbound ship gains a day. This time zone is divided into literal zones MIKE and YANKEE. The eastern half of zone 12 is designated MIKE (-12), and the western half is designated YANKEE (+12).

Now we come to a very important point in our discussion. Since MIKE and YANKEE are two parts of a single zone, the time in MIKE and YANKEE is always the same. When the IDL is crossed from either direction, the day must change. Since we have already established that there is a l-hour difference between each of the 24 time zones, it is clear that there is always a situation where it is a day earlier or later in one part of the world than it is in another. The primary point to remember about this zone is that it is always the same time in zone MIKE as it is in zone YANKEE, but it is never the same day! You can find more information on time zones in *Communication Instructions General (U), ACP 121.*

## Julian Date

The Julian date consists of seven digits. The first three digits represent the day, and the last four digits represent the hour and minutes. The first day of the calendar year is Julian 001, and each day is numbered consecutively thereafter. For example, in Julian 0311315, 031 is the 31st day of the calendar year (January 31), and 1315 is the filing time.

## PRECEDENCE

The message drafter indicates the desired writer-to-reader delivery time (speed-of-service) through the assignment of a message precedence. Although the drafter determines the precedence, the releaser should either confirm or change it. (We will talk more about the responsibilities of the drafter, originator, and releaser later in this chapter.)

Precedence is assigned according to urgency, based solely on speed-of-service, not according to the importance of the subject matter or the text. For example, an unclassified message may be assigned an IMMEDIATE precedence, whereas a Secret message may be assigned a ROUTINE precedence. In this situation, the unclassified message requires fast action or response, whereas the Secret message may not require any action at all.

The following paragraphs list the various precedence categories, their indicators, and basic definitions:

**ROUTINE (R)**— This category is assigned to all types of traffic that justify electrical transmission but which are not of sufficient urgency to require a higher precedence.

**PRIORITY (P)**— This category is reserved for messages that furnish essential information for the conduct of operations in progress. This is the highest precedence normally authorized for administrative messages.

**IMMEDIATE (O)**— This category is reserved for messages relating to situations that gravely affect the national forces or populace and which require immediate delivery to addressees.

**FLASH (Z)**— This category is reserved for initial enemy contact reports or operational combat messages of extreme urgency; message brevity is mandatory.

**YANKEE (Y)**— In addition to the four major precedence categories, an EMERGENCY COMMAND PRECEDENCE (ECP) is used within the
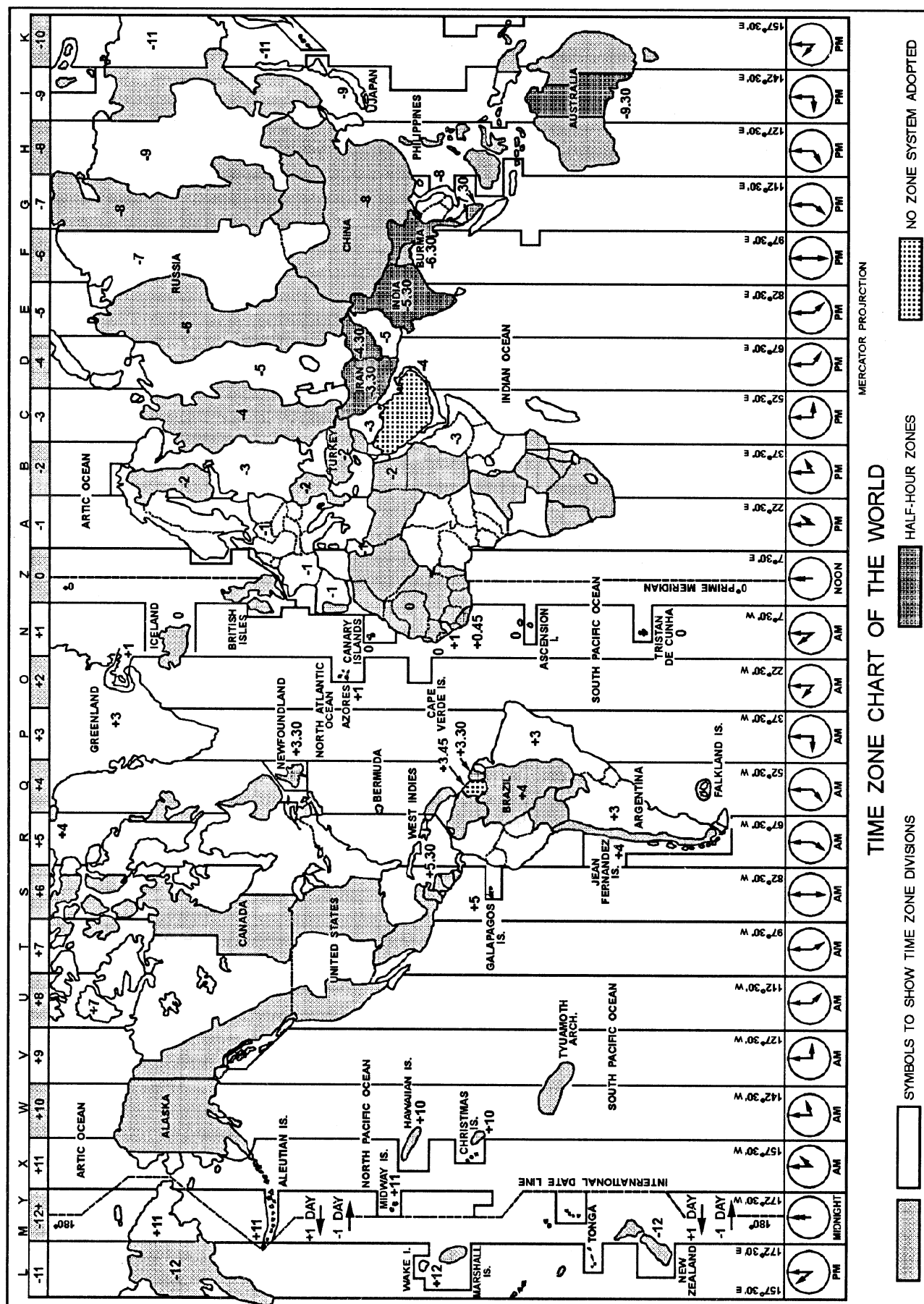
TIME ZONE CHART OF THE WORLD

Figure 2-19.—Time zone chart of the world.

RMJA0016

2-21

AUTODIN system. This ECP is identified by the precedence prosign Y and is limited to designated emergency action command and control messages.

## MESSAGE USER RESPONSIBILITIES

A message user is any individual authorized to draft, release, and/or process electronically transmitted messages. There are certain responsibilities associated with the origination of a message. These responsibilities are separate and distinct and concern the following parties:

- Originator;

- Drafter; and

- Releaser.

Occasionally, the responsibilities may overlap, especially if one person is serving a dual capacity. For example, communications officers may occasionally draft and release messages, thus making them both drafters and releasers.

### ORIGINATOR

The originator is the authority (command or activity) in whose name the message is sent. The originator is presumed to be the commanding officer of the command or activity. Most often, the originator and the releaser are one and the same.

In some cases, the drafter, releaser, and originator are all the same person. For example, if the commanding officer drafts a message for transmission, he or she is the drafter as well as the releasing authority for the activity in whose name the message is sent.

### DRAFTER

The drafter is the person who actually composes the message. In accordance with NTP 3, the drafter is responsible for:

- Proper addressing and using plain language address (PLA) designators correctly;

- Clear, concise composition;

- Selecting the precedence;

- Ensuring the proper format;

- Assigning the proper classification; and

- Ensuring the application of proper downgrading and declassification instructions to classified

messages, except those containing Restricted Data or Formerly Restricted Data.

### RELEASER

The releaser is a properly designated individual authorized to release messages for transmission in the name of the command or activity. The releasing individual ensures that the drafter has complied with the requirements contained in NTP 3. In addition to validating the contents of the message, the signature of the releaser affirms compliance with message-drafting instructions. The signature of the releaser authorizes the message for transmission.

After a message has been properly released, it is delivered to the telecommunications center (TCC) for transmission. The DTG is normally assigned here. Proper transmission, receipting, and filing procedures are done by the communications personnel.

An important point that you should remember about the DTG is that it is assigned for identification and file purposes only. It is not used to compute message processing time.

## MESSAGE READDRESSALS

If you receive or send a message and later determine that another activity may need to act on or know about the information in the message, you can readdress the original message to that activity. If you receive a copy of a message as an "information addressee," you can only readdress the original for information purposes.

Use a short form or long form, depending on how long ago the original message was sent. For both the short form and long form, you must:

- Fully identify the message you are readdressing.

- Enter the new addressee(s).

- Enter the original message originator.

- Include the original date-time group.

- Use the Process Sequence Number (PSN), if contained in the original message.

If the original message was sent within the last 60 days, use the short form to readdress it. Messages are held in the message center file for up to 60 days. On the short form, enter the *from, to,* and *information addressees* in the fields provided. Send the short form to the message center where it will be combined with the text of the original and then sent.

The short form readdressal is always unclassified. However, it must state the classification of the readdressed message.

Messages over 60 days old are routinely deleted from the message center files. If the original message to be readdressed is more than 60 days old, use the long form. Enter the *from, to,* and *information addressees* in the fields provided. Unlike the short form, you retype the entire message. Classify the long form the same as the original message.

When a sectionalized message is readdressed, each section of the message must be readdressed separately. The headerlines and addressees must be the same on each readdressal. The PSN must match that of the section being readdressed, but the respective section number is omitted. Each section of the readdressed message should have the same date-time group.

The precedence of the readdressal message maybe lower, the same as, or of a higher precedence than the original message when deemed operationally imperative by the readdressal authority.

General formatting instructions and preparation guidance are available in NTP 3. Message readdressal procedures may vary slightly at different TCCs. The required procedure may be verified through the local TCC.

## MINIMIZE MESSAGES

Military telecommunications systems tend to become overloaded during an emergency. Naturally, it becomes necessary to reduce unnecessary traffic volume to clear user circuits for essential traffic. This reduction in traffic is accomplished by use (usually by message) of the word "MINIMIZE." Minimize means **"It is now mandatory that normal message and telephone traffic be reduced drastically so that vital messages connected with the situation indicated will not be delayed."**

A message ordering minimize consists of the word "MINIMIZE" followed by the area affected (scope), reason, and duration of the minimize condition (when known). Minimize messages must be brought to the immediate attention of the leading communications petty officer (LPO) and the communications officer.

The Chief of Naval Operations (CNO), fleet commanders in chief, and area coordinators are authorized to impose minimize conditions on users of naval communications systems. Subordinate commanders may impose minimize over elements of

their commands only with prior permission from one of the three authorities just mentioned.

During minimize conditions, FLASH and IMMEDIATE traffic should be restricted to a maximum of 100 and 200 words, respectively. Message releasers are also kept to a minimum and must be specifically designated in writing. We briefly discuss additional minimize guidelines later in this chapter. NWP 4 (NWP 6-01) contains information pertaining to the types of normal, environmental, and supply traffic that may be sent over normal channels and circuits during minimize.

## SERVICE MESSAGES

Service messages are short, concise messages between communications personnel. These messages have the authority of an official communication and must receive prompt attention. If the action requested in a service message cannot be accomplished within a reasonable time, the station originating the service message should be notified. Service messages are normally assigned a precedence equal to the message being serviced.

Service messages deal with many topics. You will find that most deal with corrections, repetitions, broadcast reruns, and misrouted or missent messages. You must remember that a service message should be promptly dealt with and retained until all actions concerning it have been completed. Once action is complete, it is good practice to attach a copy of the service message to the serviced message when it is filed, or mark it with the DTG of the service(s).

Requests for information through service messages should be as brief, concise, and accurate as possible. Careful attention to detail and the use of proper operating techniques by communications and crypto personnel will reduce the number of service messages required.

Service messages are normally prepared in abbreviated plaindress format and may be assigned sequential reference numbers. (We discuss plaindress messages later in this chapter.) The service message number immediately follows the abbreviation "SVC" in the message text. If used, sequential service reference numbers may continue throughout the calendar year. When you reply to a service message received with a reference number, the text of the reply should refer to the number. For example:

UNCLAS SVC //N00000// ZUI SVC 0245 RUEDCSA 1234 1921600

2-23

This example is a service message inviting attention (ZUI) to a previous service message with a reference number of 0245. Occasionally, you will see the acronym COSIR in a service message text, which means "Cite Our Service in Reply." Authorized operating signals are used to the greatest extent possible in service messages, but clarity must not be sacrificed for brevity.

The security classification is the first word of all service message text. This is followed by the abbreviation "SVC." If the service message requires special handling, the special-handling designator follows the security classification. For example:

```
UNCLAS SVC or SECRET SPECAT SIOP ESI SVC
```

A service message may quote the textual content of a classified message or refer to the classified message in a manner that reveals textual content. In this case, the service message must be assigned the same classification as the classified message being serviced. You can find detailed information on service messages in *Automatic Digital Network (AUTODIN) Operating Procedures,* JANAP 128.

## Tracer Messages

Tracer messages are special types of service message. Tracers are sent to determine the reason for excessive delay or nondelivery of a message previously sent. Normally, tracer requests are initiated by a message originator or addressee. However, a situation may dictate that tracer action be initiated by the originating communications station, the relay station, or the communications station of the addressee.

Tracer action continues on a station-to-station basis until the cause of delay has been determined. Upon receipt of a tracer, a station should examine its records for the time of receipt and transmission of the message being traced. This information is compiled and transmitted with the tracer action to the preceding station(s) and to the station that originated the tracer. The station that caused the delay or nondelivery must cite the reason and provide a summary of corrective action in the report.

Tracer action requests must be initiated as soon as the discrepancy is discovered. Action must be initiated no later than 4 days after the original time of transmission for a tactical addressee. For nontactical addressees, action must be initiated no later than 30 days from the original time of transmission. In-station records, files, logs, and tapes must be retained beyond the required retention limit if tracer action is in progress prior to the expiration date. You can find detailed information concerning tracer action in JANAP 128.

## Termination Request Messages

Ships send termination request messages to establish circuits with a NCTAMS or NAVCOMTELSTA on a limited or full-time basis. A termination request message must be sent to the cognizant NCTAMS at least 48 hours prior to activating the requested termination. If the ship has a requirement for a full-time termination, it will be assigned a routing indicator by the cognizant NCTAMS. NTP 4 contains detailed information pertaining to termination requests and formats.

## Communications Guard Shift Messages

Communications guard shift (COMMSHIFT) messages are required when a command shifts its guard from one broadcast or servicing communications center to another. When possible, the shift takes effect at 0001Z of the new radio day. When broadcasts are shifted, an overlap period before and after the effective time is observed to ensure continuity of traffic. The command guards both broadcasts during the overlap period.

COMMSHIFT messages are sent to the NCTAMS of the communication areas from which the old and the new broadcasts originate. COMMSHIFT messages are necessary because of operational considerations or changes in the deployment schedule of a ship. These messages are necessary when a command needs to effect a shift at a time other than that indicated by its movement report. Detailed information concerning communications guard shift messages and formats is contained in NTP 4.

## Broadcast Screen Requests

Broadcast screen requests (BSRs) are service messages to request the rerun (ZDK) of missed or garbled messages. BSRs are sent to the Broadcast Keying Station (BKS) or to the designated broadcast screen ship that is responsible for the broadcast channel. NTP 4 provides detailed information and prescribes proper format for drafting a BSR.

## COMMSPOT Reports

COMMSPOT reports are used to advise of any situation that might cause significant disruption of

tactical communications. These reports are submitted by all ships and nonterminated units when unusual communications difficulties are encountered. COMMSPOT reports must be submitted as soon as unusual communications difficulties are experienced to minimize further deterioration of the communications situation.

## COMMUNICATIONS CENTER FILES

Every message handled by a ship or communications station is placed in one or more files. Some files are maintained by all ships and stations. Other files are optional and are maintained only to fill the needs of a particular ship or station.

### COMMUNICATIONS CENTER MASTER FILE

The communications center master file is the heart of the filing system. This file contains a copy or filler of every message sent or received by your command. Messages or fillers must be filed in DTG order to facilitate speed in locating messages. Those messages not having DTGs should be filed behind messages of the same date. Separate incoming and outgoing communications center master files maybe maintained.

### CRYPTOCENTER FILE

The cryptocenter file contains a copy of each Top Secret, SPECAT (less SIOP-ESI), and messages designated for special privacy, regardless of classification. Tight Control (TICON) and NATO messages must have their own files. Fillers for messages in this file must be placed in the master station file.

### SPECAT SIOP-ESI FILE

The SPECAT SIOP-ESI file contains the master copy of all SIOP-ESI messages received by the communications center. Fillers for these messages must be placed in the master station and cryptocenter files.

### BROADCAST FILE

The broadcast file contains a copy or filler of each message transmitted or received by the broadcast method. This file must be stored in accordance with the highest classification of the information contained. Top Secret and SPECAT messages addressed to the command must be filed in their appropriate files and a filler for these messages placed in the broadcast file.

### STATION FILE

The station file is divided into two parts: communications center master file and visual station file. With the exception of broadcast messages, the master file contains the circuit or "as is" copy, including any message endorsements, of all messages transmitted, received, or relayed by the communications center. Narrative visual messages or fillers must be filed in the communications center master file.

### GENERAL MESSAGE FILE

The general message file contains copies of all effective general messages that require retention based on the communications center's current guard list. This file is subdivided by general message title (such as ALNAV, ALCOM, NAVOP), and messages are filed in serial number order instead of DTG order. An example of a general message serial number is ALNAV 10/96. This indicates that it is the 10th ALNAV sent in 1996.

The individual file is marked with the classification of the highest classified message contained therein. The classified files may be segregated by security classification if desired. If a general message is canceled during the current year, the message may be destroyed, but a filler must be placed in the file to identify and indicate the disposition of all current-year general messages.

### FACSIMILE FILE

The facsimile file contains a copy of all transmissions processed by facsimile equipment. A filler for all facsimile messages must be placed in the communications center master file.

### COMMERCIAL TRAFFIC FILE

The commercial traffic file contains messages sent by commercial systems in accordance with *Fleet Communications (U),* NTP 4. This file is maintained by the commercial traffic clerk.

### EMBARKED COMMAND FILE

The embarked command file is maintained by the embarked commander's staff. When embarked commanders depart their flagships, they may require

that their files accompany them. Therefore, the embarked command file is maintained separately from the flagship file. Flagship communications personnel are responsible for processing outgoing and incoming messages for the embarked staff.

## NATO/ALLIED FILES

Classified messages of foreign origin must be provided the same protection as U.S. messages of equivalent classification. Foreign Restricted messages, for which there is no U.S. equivalent, must be protected the same as U.S. Confidential messages, except that Restricted messages do not have to be stored in a security container. You can find U.S. equivalent and foreign classifications in the *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1, hereinafter called the *Security Manual.*

NATO classified messages may not be filed with U.S. classified message. However, NATO classified message files may be stored in the same storage area with U.S. messages provided that the NATO files are clearly marked as such.

## FILE FILLERS

Because of repeated reference to previously sent message traffic, you must be able to locate all messages easily and quickly. Therefore, you must always return a message to the same file from which it was removed and in the proper filing order. When you remove a message from a file, always insert a filler, or tickler, in its place.

Fillers are locally prepared forms that identify the message by the original DTG, the message originator, information as to where the message is located, and the personal sign of the person removing the message from the file and completing the filler. For readdressal messages, a filler is made for each readdressal date-time group. The message itself is filed under the original date-time group. Figure 2-10 shows an example of a message filler, or tickler.

## FILE MAINTENANCE

Messages and fillers are filed in ascending date-time group order. The earliest message of the radio day (raday) will be at the bottom of the file. Automated systems print the DTG of each message on the lower right-hand corner of each message. For messages processed on nonautomated systems, the DTG should



Figure 2-10.—Example of a message filler.

also be printed on the lower right-hand corner. This aids personnel in easily locating messages in the files. When a message is removed from a file, it is important that it be refiled as soon as possible.

The importance of maintaining well-kept files and of moderating among the various watch sections cannot be overemphasized. Maintaining accurate files and records and observing proper procedures contribute to an efficient shipboard or shore communications organization. You should be aware that different ships and stations may do basic procedures in slightly different ways. All commands, however, must conform to the requirements contained in communications operating instructions and publications.

## RETENTION OF FILES

Communication logs and files are retained by a communications center for a specified time period, as shown in table 2-1. After the time period indicated, the logs and files should be destroyed either by burning or shredding. Because of the volume of message traffic processed, logs and files can take up significant space in the message center; therefore, they should be destroyed in a timely manner.

Table 2-1.—Retention Period of Logs and Files

| FILE/LOG | RETENTION PERIOD |
| --- | --- |
| Broadcast | 24 Hours |
| Card | 30 Days |
| Central message log | 30 Days |
| Circuit (teleprinter) | 5 Days |
| Commercial traffic | 12 Months |
| Communications center master (Either paper or LDMX/NAVCOMPARS journal tapes) | 30 Days |
| Cryptocenter file | 2 Years |
| Cryptocenter destruction log | 2 Years |
| Facsimile | 60 Days |
| General Message | When Canceled |
| Intelligence summaries | 10 Days |
| Messages incident to distress or disaster | 3 Years |
| Messages incident to or involved in any complaint for which the command has been notified | 2 Years |
| Messages of historical or continuing interest | Permanently |
| Meteorological maps and summaries | 2 Days |
| Monitor rolls and message tapes | 24 Hours |
| SPECAT SIOP-ESI file | 60 Days |
| TOP SECRET control log | 60 Days |
| Watch-to-watch inventory | 30 Days |

## COMMUNICATIONS PLANNING

The primary objectives of communications planning are:

- To provide for effective connectivity to support the exercise of command and the exchange of essential information; and

- To advise the commander of the implications of communication capabilities and limitations for the operation plan and its execution.

The communications plan has to consider reliability, security, and speed. The communications planner chooses facilities and methods that will best satisfy operational requirements. The plan provides for the command and control capability by which the operation will be controlled and directed.

To be effective, the communications planner needs comprehensive knowledge of the organizational structure established for the operation and the capabilities and limitations of the communications and command center facilities available to the force.

## COMMUNICATIONS REQUIREMENTS

The operational tasks assigned to various units require radio nets that link units engaged in the same activity or task. Communications circuits follow the command lines of the task unit or contribute to its tactical effectiveness by providing for essential information exchange. These considerations provide the essential elements for determining communications requirements.

## PROTECTION OF COMMUNICATIONS

Enemy interception and disruption of communications are of primary concern to any communications planner. Every facet of communications facilities, methods, and procedures needs to be examined in terms of security, vulnerability to deception, and the electronic protection (EP) required for maximum protection.

### Communications Security

Security is the safeguarding of information. As it pertains to communications, security is usually referred to in terms of communications security (COMSEC) and signal security (SIGSEC). Security will be discussed in more depth in chapter 3. Various devices and procedures are used to increase security, including:

- **Authentication—** A security measure designed to protect communications systems against acceptance of false transmissions or simulations by establishing the validity of a transmission, message, or originator.

- **Codes—** Any system of communication in which arbitrary groups of symbols represent units of plain text. Codes are often used for brevity and/or security.

- **Ciphers—** Any cryptologic system in which arbitrary symbols or groups of symbols represent units of plain text.

- **Radio Silence—** A condition in which all or certain radio equipment is kept inoperative (frequency band and/or types of equipment are specified).

- **Monitoring—** The act of listening, carrying out surveillance on, and/or recording the emissions of one's own or allied forces for the purpose of maintaining and improving procedural standards and Security.

- **Identification Friend or Foe (IFF)—** A system using electromagnetic transmissions to which equipment carried by friendly forces automatically responds. For example, by emitting predetermined IFF pulses, friendly forces can distinguish themselves from enemy forces.

### Communications Deception

Communications deception, part of the field of tactical deception, is the use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system.

### EA and EP

Electronic attack (EA) is that division of electronic warfare (EW) involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Enemy EA concerns the communications planner because overcoming enemy jamming and deception imposes certain restrictions on general communications operations procedures.

Electronic protection (EP) is that division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite an enemy's use of electronic warfare. The planner must be aware of EP capabilities available.

### THE COMMUNICATIONS PLAN

The communications plan satisfies the communications requirements of an operation. It specifies circuits, channels, and facilities to be used and stipulates the policies and procedures that are applicable. The plan is, in effect, an assignment of communications tasks to be performed by subordinate commanders or by supporting commands.

The planner first establishes requirements for communications and then determines the best means for satisfying them. This process may reveal shortages or inadequacies in what is available. If inadequacies are identified, it may become necessary to share circuits or facilities, as well as merging or consolidating requirements. All possibilities should be considered to support valid operational requirements.

In planning communications, the planner must evaluate such factors as the performance, capabilities, and capacities of systems, facilities, and personnel. These factors are merely guides and averages. They represent the sum result of experience in previous similar situations, and are considered only after any local factors are determined. These factors change from time to time and must all be available for final determination of communications requirements.

## TELECOMMUNICATIONS SERVICE REQUEST (TSR)

When a command requires additions, deletions, or changes in existing Defense Communications System (DCS) circuits, it must initiate a TSR. The submission of a TSR is not a simple process and requires research and planning. The Defense Information Systems Agency (DISA) publishes a publication called *Submission of Telecommunications Service Request,* DISA CIRCULAR 310-130-1, that provides instructions for preparing and submitting TSRs. New, increased, or updated services are expensive and require substantial justification.

The increasingly high cost of telecommunications support, especially leased services, has resulted in the high visibility of communications programs at all levels of government. This fact underscores the need for managerial awareness and improved life cycle documentation of telecommunications resources.

Planning and developing a responsive naval telecommunications system requires early identification and consideration of user requirements. Programming is required to obtain necessary resources. Normally, these requirements should be defined and submitted at least 2 years in advance to permit timely system planning and programming.

## TELECOMMUNICATIONS SERVICE ORDER (TSO)

The TSO is the authorization to start, change, or discontinue circuits, trunks, links, or systems. It is used to amend previously issued TSOs and to effect administrative changes.

The basic circuit design information for all new or changed circuits will be provided by the TSO. The TSO may also be used as the authority to procure specific devices and ancillary equipment necessary to install the circuit or services designated.

## FREQUENCY MANAGEMENT

Over the last quarter century, electronics has pervaded virtually every facet of our life. High-tech electronic devices, especially those that radiate, make constant use of the electromagnetic spectrum.

The term "electromagnetic spectrum" refers to the natural vibrations that occur when a force is applied to a substance. These vibrations occur with various speeds and intensities. The speed at which they occur is called frequency, and the distance between each vibration is called wavelength. Frequency and wavelengths are discussed in a later module.

### Spectrum Management

A great invention in the 19th century ultimately led to the need for spectrum, or frequency, management. This invention was the wireless or, as we know it today, the radio. At first, there were only two radio frequencies—50 kilohertz (kHz) and 1000 kHz. Today, the spectrum is recognized by international treaty to extend up to 3000 gigahertz (GHz). The development of radar, satellites, and other technologically advanced systems and their subsequent demands on the frequency spectrum have contributed to the need for frequency management.

### Frequency Allocation

The Department of the Navy will obligate no funds for equipment until a frequency allocation has been obtained. This means that all actions necessary to establish a frequency band for a specific item must be completed and approved prior to budgeting funds.

The allocation approval authority considers the type of service the item will provide and the classification of the emission. This authority also enforces rules and regulations and compliance with technical standards. The approval authority also ensures the compatibility of emerging equipment with other equipment operating in the same electromagnetic environment.

Interservice frequency coordination is another important consideration. It reduces the potential for harmful inteference if more than one service develops similar items that will operate in the same band. The coordination is the responsibility of the Chief of Naval Operations (CNO), working through the United States Military Communications Electronics Board (USMCEB).

### Frequency Assignment

Frequency assignment is the process of authorizing a system or equipment to operate on a discrete frequency (or frequencies) and within a specified set of constraints. Examples of constraints are power, emission bandwidth, location of antennas, and operating time.

Authority for using radio frequencies by Navy and Marine Corps activities within the United States and

Possessions (US&P) is obtained from the Administrator, National Telecommunications and Information Administration (NTIA), Washington, D.C.

The CNO establishes overall policy for spectrum management within the Department of the Navy. Authority for using radio frequencies by Navy and Marine Corps activities within the area of responsibility of a unified or specified commander is obtained from the Joint Chiefs of Staff through the USMCEB. Within the Department of the Navy, the Naval Electromagnetic Spectrum Center (NAVEMSCEN) authorizes frequency assignment applications and ensures all prerequisites are completed.

## SPECIAL-HANDLING MARKINGS

Certain types of messages require special-handling markings in addition to that provided by the security classification. Among these markings are such designations as Caveat, Restricted Data (RD), Formerly Restricted Data (FRD), LIMDIS, FOUO, EFTO, SPECAT, PERSONAL FOR, NATO RESTRICTED, and ALLIED RESTRICTED.

### Caveat Messages

When used with special-handling instructions, the word "caveat" means a warning by authoritative orders that directs or imposes one to protect an element, usually special message traffic.

### Restricted Data and Formerly Restricted Data

The marking "Restricted Data" (RD) is applied to all data concerned with the design, manufacture, or use of nuclear weapons. Also included in this category is the special nuclear material used in energy production.

The marking "Formerly Restricted Data" (FRD) pertains to defense information that has been removed from the RD category but must still be safeguarded as classified defense information. FRD material cannot be released to foreign nationals except under specific international agreement.

### LIMDIS (Limited Distribution)

The LIMDIS designator is applied only to classified messages which, because of the subject matter, require limited distribution within the addressed activity.

### For Official Use Only (FOUO)

FOUO is the designation used on official information not requiring a security classification but which must be withheld and protected from public release. Unclassified messages containing FOUO information must have the abbreviation "FOUO" after the designation "UNCLAS."

### Encrypt for Transmission Only (EFTO)

Certain categories of unclassified messages may be identified as having potential value if subject to analysis, but do not meet the criteria for security classification. The special designation "EFTO" was established to protect these unclassified messages during electrical transmission.

EFTO is not required on unclassified messages addressed exclusively among Navy, Marine Corps, and Coast Guard commands. EFTO is authorized for use within the Department of Defense, including the National Security Agency. However, EFTO is required on FOUO messages addressed to DOD activities outside the continental United States. Bear in mind, however, that just because information is FOUO, it is not automatically EFTO, and vice versa.

As we mentioned earlier, EFTO is a transmission marking for unclassified messages. FOUO markings, however, define a certain category of information requiring special handling. Neither FOUO nor EFTO markings are security classifications; both are special-handling designations. You can find detailed information on EFTO and FOUO markings in *Basic Operational Communications Doctrine (U),* NWP 4 (NWP 6-01).

### SPECAT

The SPECAT marking means special category. SPECAT messages are classified messages identified with a special project or subject. SPECAT messages require special-handling procedures in addition to the handling procedures for the security classification of the message. There are four SPECAT categories:

- SPECAT;

- SPECAT EXCLUSIVE FOR (SEF);

- SPECAT Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI); and

- PSEUDO-SPECAT.

SPECAT and SPECAT EXCLUSIVE FOR messages must be at least Confidential. SPECAT SIOP-ESI messages are always Top Secret. PSEUDO-SPECAT messages are normally unclassified messages that require limited distribution. Examples of PSEUDO-SPECAT messages include AMCROSS messages, urinalysis test results, and HIV test results.

SPECAT messages are handled only by those personnel who are authorized by the commanding officer in writing to view them. The types of information assigned SPECAT and handling procedures can be found in NWP 4 (NWP 6-01) and in *Fleet Communications (U),* NTP 4, respectively.

## PERSONAL FOR

PERSONAL FOR is the marking applied when message distribution must be limited to the named recipient. Only flag officers, officers in a command status, or their designated representatives may originate PERSONAL FOR messages.

## NATO RESTRICTED

The United States does not have a security classification equivalent to NATO RESTRICTED. NATO messages classified as restricted must be safeguarded in a manner similar to FOUO messages. Messages originated by NATO must be handled in accordance with *NATO Security Procedures (U),* OPNAVINST C5510.101.

## ALLIED RESTRICTED

The United States does not have a security classification equivalent to ALLIED RESTRICTED. However, these messages must be handled in the same manner as Confidential messages. U.S.-originated messages containing ALLIED RESTRICTED information are marked as "Confidential" immediately following the security classification.

## MINIMIZE CONSIDERED

During an actual or simulated emergency, it may become necessary to decrease the amount of record and/or voice communications on military telecommunications circuits. When this occurs, it is called MINIMIZE. In essence, all messages that are not urgent will not be transmitted. Those messages that concern a mission or safety of life are considered imperative and, therefore, require transmission during minimize.

The same criteria pertaining to minimize conditions noted earlier in this chapter still apply. The releasing officer must review and decide on the message's merit, which means the message will be sent, either electrically or by another means. When a message is released, it must include the words "MINIMIZE CONSIDERED" and "RELEASED BY."

Messages that will not be sent electrically during minimim periods should be returned to the originator with the reason for their return. Normally nontransmitted messages will be sent via U.S. mail if they meet established security guidelines.

## JCS EMERGENCY ACTION MESSAGES

Joint Chiefs of Staff (JCS) Emergency Action Messages (EAMs) contain key instructions or information from high-level authority and have predetermined formats (pro forma). Such messages are transmitted by various communications systems and normally carry FLASH (Z) precedence. They are vital messages of an extremely time-sensitive nature, and rapid processing is mandatory to achieve the fast reaction required by their content. Usage and handling procedures are issued by the JCS to those who have a need to know.

SPECAT messages come in two variations. One type includes both the general SPECAT and the SPECAT Single Integrated Operational Plan—Extremely Sensitive Information (SPECAT SIOP-ESI). This type of SPECAT message is associated with code words or projects. For example, a Secret message whose subject matter deals with a special project entitled "TACAMO" would have a classification line reading SECRET SPECAT TACAMO. SPECAT SIOP-ESI messages are always classified Top Secret. SPECAT (less SIOP-ESI) messages must be classified at least Confidential.

The other type of SPECAT message is SPECAT EXCLUSIVE FOR (SEF). SEF is used only within the naval community for highly sensitive matters, high-level policy, or when politically sensitive information is to be passed only to a particular individual. The classification line would then contain the name of that individual. For example, a Secret message destined exclusively for Admiral W. T. Door would read:

SECRET SPECAT EXCLUSIVE FOR ADM W. T. DOOR //N00000//

SEF messages are reserved for use by flag officers and officers in a command status. These messages are not intended for use in operational matters, and they

may not be readdressed nor referenced in other narrative messages.

SPECAT messages are handled only by those personnel who are authorized to view them as approved in writing by the commanding officer.

## NAVAL WARFARE PUBLICATIONS LIBRARY

The naval warfare publications library (NWPL) is the designation assigned to that group of communications and operational publications designated as part of the publication allowance for the command. These publications contain required procedures, signals, and other information of an operational or mission-essential nature. They may also include information involving safety. The NWPL provides for the central administration and maintenance of communications and operational publications. These publications include, but are not limited to:

- Naval telecommunications publications (NTPs);

- Naval warfare publications (NWPs);

- Fleet exercise publications (FXPs);

- Allied tactical publications (ATPs);

- Allied exercise publications (AXPs);

- USN addenda to allied publications; and

- Miscellaneous allied publications.

The objective of central administration of naval warfare publications (NWPs) is to ensure that these publications are correct and readily available for their intended use. Some NWPs contain information that is necessary for the proper performance of individual duties and is important for individual professional development. Therefore, NWPs must be readily available for use by individuals with a duty-related need or a general professional need for the information.

## NAVAL WARFARE PUBLICATIONS CUSTODIAN

The responsibility for managing the NWPL is assigned to an officer or senior petty officer who is responsible to the executive officer, department head, or division officer. This assignment is a collateral duty, and the person assigned is known as the naval warfare publications custodian (NWPC). This person is responsible for the overall administration and security of the NWPL in accordance with the *Naval Warfare Documentation Guide,* NWP 0 (NWP 1-01).

## NAVAL WARFARE PUBLICATIONS LIBRARY (NWPL) CLERK

The NWPL clerk is a person assigned by the NWPC. The clerk is responsible for the upkeep and maintenance of the library. The NWPL clerk maintains all records and receipts in the central file, orders all necessary publications and changes thereto, and enters all changes and amendments to publications physically held in the NWPL. The clerk reports all matters of concern to the library custodian.

## NWPL ADMINISTRATION

The NWPL custodian issues publications to holders and short-term users. A holder is a person who has permanent subcustody of a publication under the central control of the NWPL. The holder is responsible for maintaining the publication, entering all changes and amendments, and providing adequate security. A user is a person who checks out a publication for temporary or short-term custody.

Signature custody and disclosure records for classified material are maintained as required by the Security Manual. Signature custody of unclassified publications is not required. However, the records of the NWPL should provide an up-to-date location of publications that have been issued to holders or checked out to users. Where signature custody is not required, a locator card maybe used in place of a catalog card to check out publications to users.

## NWPL MAINTENANCE

Several basic files are used in maintaining the NWPL. One is the custody file, which contains a NWPL Catalog Card, OPNAV Form 5070-11 (figure 2-11), for each naval warfare publication on allowance or on board. The purpose of this file is to maintain an up-to-date record of the holder and location of each publication. This record also helps keep track of entries and changes to the publication. The catalog card can also be used as a custody card and as a destruction record. When used as a record for security purposes, it must be retained as required by the *Security Manual.*

The administrative file, sometimes called the transaction file, contains designation letters for custodian, local allowance/inventory sheets, the directives file, responsibility acknowledgment forms,

| SHORT TITLE NTP 4 ( ) | COPY Documents On Hand [m]1 [p]2 []3 []4 []5 []6 | | | | | CLASSIFICATION OF PUBLICATION | | | |
|---|---|---|---|---|---|---|---|---|---|
| LONG TITLE | | | | | | EFFECTIVE DATE | | | |

| CHANGE OR CORRECTION | DATE OF ENTRY BY COPY NUMBER | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| CHG #1 | | | | | | | | | | |
| CHG #2 | | | | | | | | | | |
| MSG CORR 1/1 | | | | | | | | | | |
| | | | | | | | | | | |

NOTES: MSG CORR entered into a microfiche copy of a publication be placed into the envelope with the copy and annotated on the envelope.

ENTRY DATE will be written into each column for each copy of the publication receiving change or correction.

**OPNAV FORM 5070-11 (11-57) BACK**

| | DEPOSITION OF PUBLICATION | | | | | | |
|---|---|---|---|---|---|---|---|
| COPY NO. | HOLDER (Signature) | LOCATION | REC'D. DATE | RETURN DATE | DESTRUCTION | | |
| | | | | | DATE | AUTHORITY | |
| 1&2 | NWPL Custodian's Sig | NWPL | *1 | | *5 | *6 | |
| 1 | Subcustodian's Sig | RADIO | *2 | *3 | | | |
| | | CENTRAL | | | | | |
| 1 | NWPL Clerk's Sig | NWPL | *4 | | | | |
| | | | | | | | |

NOTES: *1. Date copy received into library.
*2. Date subcustodian received copy.
*3. Date subcustodian returned copy to library.
*4. Date publication received by library.
*5. Date copy destroyed.
*6. Authority cited for destruction of copy.

RMJA0018

Figure 2-11.—NWPL Catalog Card.

publication notice route slips, destruction records, inspection documentation letters, and copies of all correspondence pertaining to naval warfare publications. Included in the administrative file is the Change Entry Certification form, OPNAV 5070/12, shown in figure 2-12. This form is filled out by the holder of the applicable publication. Material in the administrative file must be retained for 2 years.

## NWPL BINDERS

Binders for U.S. naval warfare publications are color-coded according to their security classification. The color codes are RED for Secret, YELLOW for Confidential, and BLUE for unclassified. Allied/NATO publications have white binders regardless of security classification.

| CHANGE ENTRY CERTIFICATION OPNAV 5070/12 (REV. 6-75) | | RETURN TO NAVAL WARFARE PUBLICATIONS LIBRARY | |
|---|---|---|---|
| SHORT TITLE | COPY NO. | CHANGE | EFFECTIVE DATE |

REMARKS:

*I certify that the above change or correction has been entered and the list of effective pages was checked against the contents of the basic publication, and the superseded pages and residue of the change were returned to the Naval Warfare Publications Library.*

NOTE: *Missing pages or other defects should be reported in the REMARKS space above.*

| SIGNATURE | ENTRY DATE |
|---|---|

PART 2 S/N 0107-LF-050-7061

| SHORT TITLE | COPY NO. | CHANGE | EFFECTIVE DATE |
|---|---|---|---|

REMARKS:

*I acknowledge receipt of the above change and certify that this change will be entered upon the effective date/immediately and that the superseded pages will be returned to the Naval Warfare Publications Library within five (5) working days thereafter.*

| SIGNATURE | DATE |
|---|---|

PART 1 S/N 0107-LF-050-7061                                    C-3500

Figure 2-12.—Change Entry Certification form.

## ENTRY OF CHANGES

The timely and accurate entry of changes to NWPL publications is necessary to ensure accurate, up-to-date information as well as information continuity. The NWPL clerk is responsible for making changes or corrections to NWPL publications or ensuring that holders receive. and make the changes in a timely manner.

Changes are often so numerous that all communications personnel may become involved in making them. The NWPL clerk is responsible for ensuring that all personnel making changes or corrections to NWPL publications know the proper procedures for making these changes. These procedures are a follows:

- Check the Foreword or Letter of Promulgation of the change for the effective date of the change/correction to ensure that the publication to be corrected is effective.

- Read all the specific instructions contained in the change or correction before making the entry.

- Use any dark ink EXCEPT RED for pen-and-ink entries. Red is not visible under red night lights used aboard ship.

- Type lengthy pen-and-ink corrections on a paste-in cutout. All superseded matter must be deleted in ink prior to inserting the cutout.

- Use flaps when no room exists for a cutout. When used, flaps should be attached to the binder side of the page.

- Use rubber cement or mucilage for pasting instead of glue or gummed tape.

- Make a notation in the margin adjacent to the entry after making pen-and-ink corrections, citing the source of the correction; for example, ALCOM 007/96.

After page changes are entered, a page check must be conducted and the page change and page check recorded on the Record of Changes and Corrections sheet.

Corrections to NWPL publications are issued by message when the material requires rapid dissemination. These numerical message corrections (NMCs) are normally sent as general messages. NMCs are assigned a two-number designation separated by a slant sign. The first number indicates the sequential number of the message correction to the original or revised publication. The last number is the printed change that incorporates the material. For example, NMC 7/3 is the 7th message correction and is incorporated into the publication by change 3.

## PUBLICATION NOTICE

A publication notice gives a brief summary of a new publication or change. The notice is included with each hardback copy and is furnished solely for routing by the NWPC. These notices keep all cognizant personnel informed of the changes to naval warfare publications. The notices are destroyed when no longer useful.

## WATCH-TO-WATCH INVENTORY

To ensure positive control of NWPL publications, a watch-to-watch inventory should be conducted. At the change of each watch, the watches jointly conduct a visual inventory of every publication held by the watch section. Those loose-leaf publications requiring a page check at the end of the watch must be indicated on the inventory sheet.

The signing of the watch-to-watch inventory by the relieving watch certifies that the publications were sighted, the required page checks were conducted, and that the relieving watch stander is responsible for them. Any discrepancies should be resolved prior to the relieving of the watch.

All signatures in the watch-to-watch inventory must be in ink. The inventory may be destroyed after 30 days if it is no longer needed for local reference. If watch-to-watch inventories are not required aboard ship, a daily inventory is required.

## EXTRACTS

Naval warfare publications may be extracted/ reproduced for use in training or operations of U.S. forces. All extracts must be properly marked with the security classification and safeguarded in accordance with the Security Manual.

The classification assigned to an extract is the highest classification assigned to any article, paragraph, page, or pages from which the information is taken. Guidance for allied (NATO) publications is found in their NATO letters of promulgation.

## RECEIVING NEW OR REVISED PUBLICATIONS

When new or revised publications are received, you should check the Foreword and the U.S. Letter of Promulgation for the effective status of the publication. The Foreword shows the effective status of the publication for allied usage; the U.S. Letter of Promulgation for U.S. use.

A revision to a publication can be issued that is effective for U.S. use but not for allied use. Particular care should be taken not to destroy the previous edition until the new revision is effective for allied use as well.

## ALLIED COMMUNICATIONS PUBLICATIONS

With worldwide cooperation among friendly nations and the United States, the need arose for coordinated and standardized communications. To meet this need, the allied communications publications (ACPs) were developed. The ACP series provides communications instructions and procedures essential to conducting combined military operations and communications in which two or more allied nations are involved. A Radioman's work often requires familiarity with ACPs.

## JOINT ARMY-NAVY-AIR FORCE PUBLICATIONS

Joint Army-Navy-Air Force publications (JANAPs) were developed to coordinate and standardize communications among the U.S. military services. The publication *Status of Noncryptographic JANAPs and ACPs,* JANAP 201, lists the short and long titles, content of each publication, and the current edition of JANAPs and ACPs.

## NAVAL TELECOMMUNICATIONS PUBLICATIONS

Naval telecommunications publications (NTPs) are the main communications publications in use by the U.S. Navy, Coast Guard, and Marine Corps. The NTPs include information and guidance from basic communication information (NTP 4), to frequency spectrum management (NTP 6), and commercial traffic (NTP 9), just to name a few areas of communications.

## NAVAL WARFARE PUBLICATIONS

Naval warfare publications (NWPs) incorporate the results of fleet tactical development and evaluation programs and fleet and allied (NATO) experience. NWPs also provide information about the tactical capabilities and limitations of equipment and systems. NWP 0 (NWP 1-01) provides guidance for managing the NWPL and lists the publications contained in the library.

## FLEET TELECOMMUNICATIONS PUBLICATIONS

Fleet telecommunications publications (FTPs) are the guiding doctrine of a NCTAMS for the communications area under its jurisdiction. To provide optimum communications responsiveness to fleet requirements. FTPs incorporate the unique communications procedures for the COMMAREA into a standardized fleet-oriented procedural document. FTPs are based on the NTP series.

## COMMUNICATIONS INFORMATION BULLETINS

Communications information bulletins (CIBs) are developed by each NCTAMS to provide reference information on specific tactical communications subjects. CIBs also provide communications operating personnel with communications procedural information applicable to a specific COMMAREA. NTP 4 lists the CIBs and their contents.

## SUMMARY

As you have learned from this chapter, the naval communications establishment is quite complex. We communicate not only with other U.S. naval commands, both at sea and ashore, but also with other U.S. military services and allied nations. Before the messages that you send reach their destinations, they may travel through other networks in the Defense Communications System.

We have introduced you to the basic principles of communications management, evaluation of both personnel and the work area, and duties of individual positions within the command. We have also covered various categories of messages that have both internal and external use in the message center.

This chapter has introduced you to the standard procedures associated with handling incoming and outgoing messages. Because of the volume of messages a telecommunications center processes, it is essential that communications personnel observe all the handling procedures to prevent losing or delaying delivery of messages to subscribers.

Understanding the communication plan will give you a view of the ever-changing overall plans for your ship or shore station and its requirements for mission completion.

The various publications that you, as a communicator, rely on are continually being updated. Communications is an area that is constantly changing in areas of equipment and procedures. Therefore, it is important you become thoroughly familiar with all the publications and current changes that pertain to your communications area.

The tasks of a message center are extremely important. Your understanding of the handling procedures is key to providing fast and accurate communication to the fleet.